PANDA
CLOUDSYSTEMS
MANAGEMENT

PANDA CLOUD SYSTEMS MANAGEMENT

Guía para Partners y Administradores de red

www.pandasecurity.com

PRÓLOGO
¿A quién está dirigida esta guía? Iconos.
03

INTRODUCCIÓN
Características principales. Perfil de Usuario. Actores principales.
04

JERARQUÍA DE NIVELES PARA LA CONSOLA PCSM DE ADMINISTRACIÓN
System Level. Profile Level. Device Level.
08

ELEMENTOS BÁSICOS DE LA CONSOLA PCSM
Menú general. Barra de Pestañas / Barra de Listados. Barra de Iconos / Barra de Acciones. Panel de grupos y filtros. Paneles de control.
11

FILTROS Y GRUPOS
¿Qué son los grupos y filtros? Tipos de grupos y filtros. Grupos. Filtro.
16

CÓMO ORDENAR LOS DISPOSITIVOS ADMINISTRADOS DE FORMA EFICIENTE
Enfoque general y estructura de ordenación de dispositivos...
20

LOS 8 PRIMEROS PASOS PARA COMENZAR A USAR PCSM
Creación y configuración del primer Profile. Deploy del Agente PCSM...
22

POLÍTICAS / POLICIES
¿Que son las Policies? ¿Cómo defino una System Policy? ¿Cómo defino una Profile Policy? ¿Cómo defino una Device Policy? Tipos de policies. ¿Cómo distribuyo una policy?
28

MONITORING
¿Qué es? Composición de un monitor. Creación de monitores.
31

DESARROLLO DE COMPONENTES
¿Por qué desarrollar componentes? ¿Qué requisitos son necesarios para el desarrollo de componentes? Arquitectura general de componentes en PCSM. Creación de un componente de tipo monitor. Creación de un componente de tipo Script.
35

DISTRIBUCIÓN E INSTALACIÓN CENTRALIZADA DE SOFTWARE
Objetivo de la instalación centralizada de software. Requisitos para la instalación centralizada de software...
44

TICKETING
¿Qué es el sistema de ticketing? Descripción de un ticket. Creación de un ticket. Gestión de tickets.
54

PATCH MANAGEMENT
¿Qué es Patch Management? ¿Qué parches puedo distribuir / aplicar? Distribución e instalación de parches. Auditorías.
57

CUENTAS DE USUARIO Y ROLES
¿Qué es una cuenta de usuario? ¿Qué es un rol? ¿Porque son necesarios los roles? El rol accountadmin...
64

GESTIÓN DE DISPOSITIVOS MÓVILES
¿Qué plataformas se soportan? Integración de dispositivos móviles en PCSM. Herramientas para la gestión remota de dispositivos móviles.
70

APÉNDICE A
Código fuente del componente del cap. 10.
75

APÉNDICE B
Código fuente del componente del cap. 11.
77

01. PROLOGO

Esta guía contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto **Panda Cloud Systems Management** (a partir de ahora **PCSM**).

¿A QUIÉN ESTÁ DIRIGIDA ESTA GUÍA?

Esta documentación está pensada para el personal técnico que ofrece servicios de soporte a usuarios sin conocimientos informáticos, y lo hace desde dos posibles entornos:

- ✔ Desde el departamento de IT de la empresa que desea profesionalizar el soporte técnico interno que ofrece al resto de la compañía.
- ✔ Desde el proveedor de servicios gestionados (MSP) que actualmente ofrece servicios de soporte técnico presencial o remoto, reactivo o proactivo, a sus cuentas de clientes.

ICONOS

En esta guía aparecen los siguientes iconos:

- Información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.
- Sugerencias y recomendaciones.
- Consejo importante de cara a un uso correcto de las opciones de Panda Cloud Systems Management.

02. INTRODUCCIÓN

Panda Cloud Systems Management es la solución de **monitorización y administración remota** de dispositivos **basada en la nube** para departamentos de IT que quieren ofrecer un servicio profesional y minimizar su impacto en las tareas del usuario**. Panda Cloud Systems Management** incrementa la eficiencia a través de una gestión de dispositivos centralizada y sencilla, favoreciendo a su vez la automatización de tareas. De esta forma los costes generales invertidos en dar servicio a cada cliente se ven reducidos ya que **PCSM** cuenta con:

- Nula infraestructura adicional necesaria en las instalaciones del partner y en la cuenta del cliente gracias a su servicio alojado en la Nube.
- Curva de aprendizaje muy suave para los técnicos de soporte, que le permitirá ofrecer valor desde el primer momento.
- Herramienta accesible desde cualquier lugar y en cualquier momento, facilitando las guardias no presenciales del equipo técnico y evitando desplazamientos gracias al acceso y control remoto de dispositivos.
- Automatización de tareas desencadenadas de forma automática como respuesta a alertas programadas, que previenen fallos antes de que se produzcan.

Panda Cloud Systems Management es un producto que favorece la colaboración entre los técnicos encargados de ofrecer soporte, al tiempo que minimiza o evita completamente el tiempo dedicado a interactuar con el usuario para determinar las causas de los problemas.

CARACTERÍSTICAS PRINCIPALES DE PANDA CLOUD SYSTEMS MANAGEMENT

A continuación se indican las características más importantes del producto:

Característica	Descripción
Solución basada íntegramente en la Nube	No precisa infraestructura adicional en el cliente o en el MSP / departamento de IT. Permite gestionar todos los dispositivos en cualquier momento y desde cualquier lugar.
Basada en Agente	Un **Agente** muy ligero compatible con cortafuegos y VPN NAT comunica cada dispositivo con el **Servidor PCSM**.
Detección automática de dispositivos	El **Agente PCSM** instalado en un solo dispositivo puede detectar otros dispositivos conectados a la misma red e iniciar su instalación automática.
Auditorías programadas y extraordinarias	Permite llevar a cabo un seguimiento de todos los cambios realizados en el dispositivo (hardware, software y sistema).
Gestión de licencias de software	Permite realizar un seguimiento de todo el software instalado.
Alertas y monitorización	Control del uso de CPU, memoria y disco, servicios y servidores Exchange, gráficos de rendimiento, alertas en panel, etc., y todo en tiempo real.
Creación de scripts y tareas rápidas	Permite crear scripts o descargar scripts preconfigurados de la ComStore en línea y lanzarlos de forma programada o como respuesta automática a una alerta. Todo ello con un solo clic.
Gestión de parches	Automatización del despliegue de actualizaciones y parches para el software instalado.
Despliegue de software	Despliegue del software y las actualizaciones de forma centralizada.

Continua

Característica	Descripción
Políticas	Posibilitan establecer un conjunto de configuraciones comunes para gestionar el entorno de IT de forma ágil.
Acceso remoto	Gestor de tareas, transferencia de archivos, editor de registros, símbolo del sistema, visualizador del registro de eventos, etc. Todas estas herramientas integradas permiten reparar varios dispositivos sin que el proceso impacte en la labor de los usuarios.
Control remoto	Acceso compartido al escritorio del usuario o control total. Compatible con cortafuegos y NAT.
Comunicación segura	Todas las comunicaciones entre los Agentes y el Servidor PCSM están cifradas (SSL).
Informes	Permite enviar por correo informes programados o extraordinarios. Facilita información sobre las tareas realizadas y quién las realiza, además de datos sobre el uso de los recursos realizado por los usuarios.
Entorno colaborativo	Dispone de un Ticket System que permite gestionar la asignación, el estado y la documentación de las incidencias. Facilita la creación de históricos de intervención con Device Notes y mejora la comunicación en vivo con el usuario mediante el servicio de Mensajería IM.
ComStore	Complementa y amplía las capacidades de la plataforma, al permitir la selección y descarga de los componentes necesarios en cada momento.
Gestión de dispositivos móviles (MDM)	Compatible con iOS y Android, permite monitorizar móviles y tablets, localizarlos y evitar la pérdida de datos en caso de robo o pérdida del dispositivo.

PERFIL DE USUARIO DE PANDA CLOUD SYSTEMS MANAGEMENT

Los usuarios de **Panda Cloud Systems Management** van a compartir un perfil técnico medio-alto, ya que se trata de una herramienta orientada al mantenimiento diario de dispositivos informáticos sometidos a un régimen constante de uso y cambio. Sin embargo se distinguen dos grandes grupos de usuarios de **Panda Cloud Systems Management**:

- **Técnicos pertenecientes al departamento de IT de la empresa**
  Son técnicos subcontratados o pertenecientes a la plantilla de la empresa que ofrecen un servicio de soporte a los dispositivos y usuarios de la propia empresa. Este escenario contempla la existencia de oficinas distribuidas (remotas) a los cuales los técnicos deberán acceder con herramientas de monitorización y acceso y control remoto, así como usuarios en itinerancia o que desarrollan su labor fuera de la oficina y son susceptibles de sufrir problemas en sus dispositivos.

- **Técnicos pertenecientes a un proveedor de servicios gestionados (MSP)**
  Se trata de personal técnico que pertenece a una empresa dedicada a ofrecer servicio técnico profesional a aquellas cuentas de cliente que hayan decidido externalizar o subcontratar el departamento de IT para el mantenimiento de sus dispositivos.

Componentes principales de Panda Cloud Systems Management.

- **Consola PCSM**
  Se trata de un portal web accesible a través de un navegador compatible, desde cualquier lugar y en cualquier momento, con una simple conexión a Internet.
  La mayor parte de las actividades diarias de seguimiento y monitorización se realizarán desde este portal web y a través del navegador. Es un recurso accesible únicamente a los técnicos encargados de ofrecer soporte.

- **Agente PCSM**
  Es un pequeño programa de 3 megabytes de tamaño que se instala en cada uno de los dispositivos que serán administrados. Una vez instalado el **Agente PCSM** en el dispositivo éste se volverá directamente accesible por el técnico de soporte a través de la **Consola PCSM**.

  El **Agente PCSM** admite dos modos de ejecución:

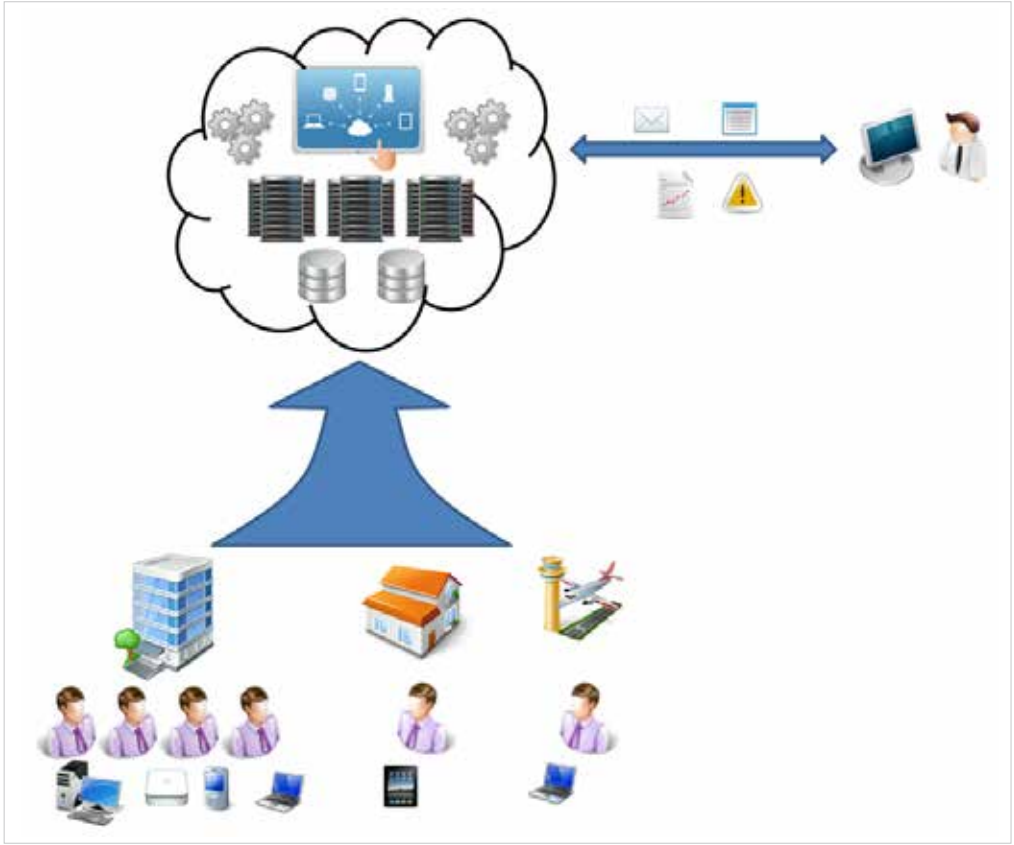
  A) Modo Usuario o Modo Monitor
  Es el modo en que se ejecuta normalmente, pensado para pasar inadvertido al usuario del dispositivo la mayor parte del tiempo y, solo puntualmente y si el administrador lo permite, podrá tener cierto acceso a algunas configuraciones particulares.

  B) Modo Administrador
  El Agente PCSM puede ser utilizado por el administrador de la red para acceder a dispositivos remotos previa introducción de unas credenciales válidas.

Instale el **Agente PCSM** en todos los dispositivos del cliente que desea administrar y también en aquéllos que utilizarán los técnicos para la administración remota.

- **Servidor PCSM**
  La **Consola PCSM**, los procesos necesarios para recoger, sincronizar y redirigir los mensajes, eventos y flujos de información generados por los **Agentes PCSM** y la base de datos que los sustenta quedan recogidos en un **Servidor PCSM** alojado en la nube, online las 24 horas del día.

  La información de estado que fluye desde cada uno de los dispositivos hacia el **Servidor PCSM** está muy optimizada, de forma que el impacto en la red del cliente es inapreciable. En el **Servidor PCSM** esta información se ordena y consolida para ser mostrada como un flujo de eventos que permitirá diagnosticar e incluso anticipar de forma eficiente los problemas de los dispositivos administrados.



ACTORES PRINCIPALES DE PANDA CLOUD SYSTEMS MANAGEMENT

- **Administrador de IT / Administrador / Proveedor de servicios gestionados / MSP / Departamento de IT /Técnico de soporte / Equipo técnico**
  Bajo esta denominación se engloban todas aquellas personas que tengan acceso a la **Consola PCSM**, independientemente del nivel de privilegios asociado a las credenciales suministradas.

  Se trata de personal técnico perteneciente al departamento de IT de la empresa que adopta **Panda Cloud Systems Management** para administrar sus propios equipos, o personal del MSP que accede a los dispositivos de clientes para su administración y monitorización.

- **Cuenta de administración PCSM / Cuenta de administración principal**
  A cada empresa que adquiera el producto **Panda Cloud Systems Management** se le hará entrega de una cuenta de administración principal. Es una cuenta con los máximos privilegios capaz de gestionar todos los recursos del producto.

En el capítulo 14 se contempla la creación de nuevos usuarios y roles en el sistema para delimitar el acceso de los técnicos de sistemas a recursos clave de **Panda Cloud Systems Management**.

- **Cuenta de cliente / Cliente**
  Una cuenta de cliente es un contrato firmado entre el proveedor de servicios gestionados y una empresa que acude a él con la intención de externalizar los servicios informáticos que requiera en el día a día.

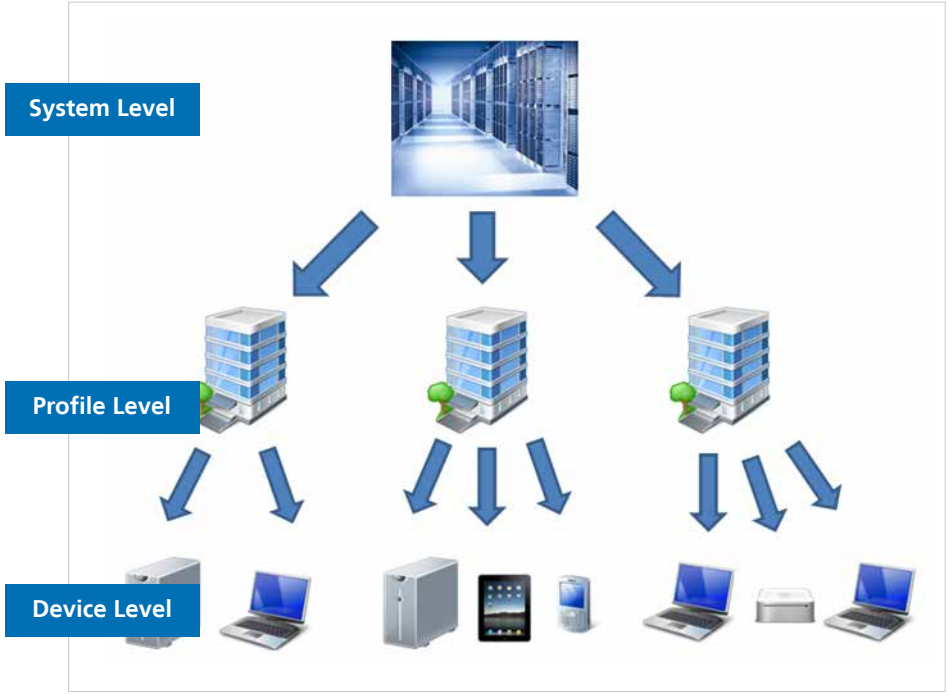
  Excepto en el capítulo 14 dedicado a la creación de usuarios y roles, en este manual una cuenta tiene un significado organizativo: para el MSP equivale a un conjunto de dispositivos relacionados entre sí por pertenecer a una misma red del cliente, y que requerirán de un mantenimiento.

- **Usuario**
  El usuario es la persona que utiliza uno o más dispositivos y que requiere soporte técnico directo del MSP o departamento de IT.

- **Dispositivo**
  Un dispositivo es un equipo informático que lleva instalado un **Agente PCSM** y que es utilizado por el usuario en su trabajo diario.

03. JERARQUÍA DE NIVELES PARA LA CONSOLA PCSM DE ADMINISTRACIÓN

Con el objetivo de separar la administración de los dispositivos de distintas cuentas de cliente y de poder reutilizar y limitar procedimientos establecidos por el personal técnico en la **Consola PCSM** y así agilizar y afinar su administración, **Panda Cloud Systems Management** establece tres entidades / niveles de agrupación / operación posibles. De la más general a la más particular son las siguientes:



SYSTEM LEVEL

¿Qué es?

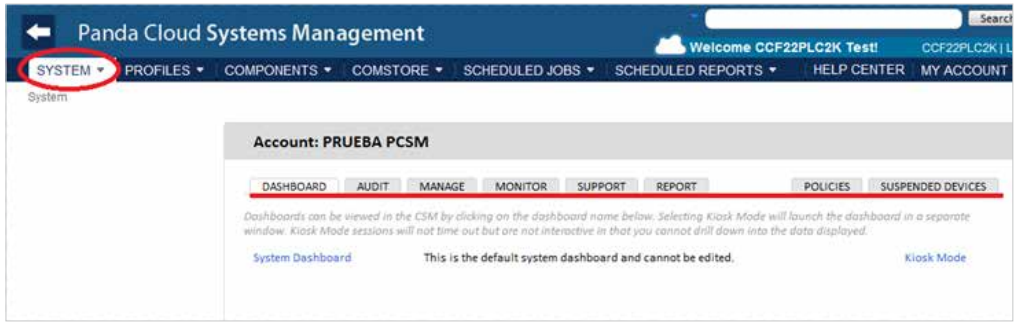
El System Level es la entidad de agrupación más general y de mayor nivel posible, siendo además única por cada MSP / departamento de IT. Agrupa automáticamente todos los dispositivos administrados por el MSP / departamento de IT pertenecientes a sus clientes y usuarios, y que tengan un Agente PCSM ya instalado.

Ámbito

Las acciones realizadas en este nivel podrán afectar a todos los dispositivos dados de alta en el sistema si bien podrán ser limitadas a un subconjunto de dispositivos mediante filtros y grupos descritos en el capítulo 5.

Acceso

El acceso a los recursos de la entidad System se realizan desde el Menú General, System.



Funcionalidad

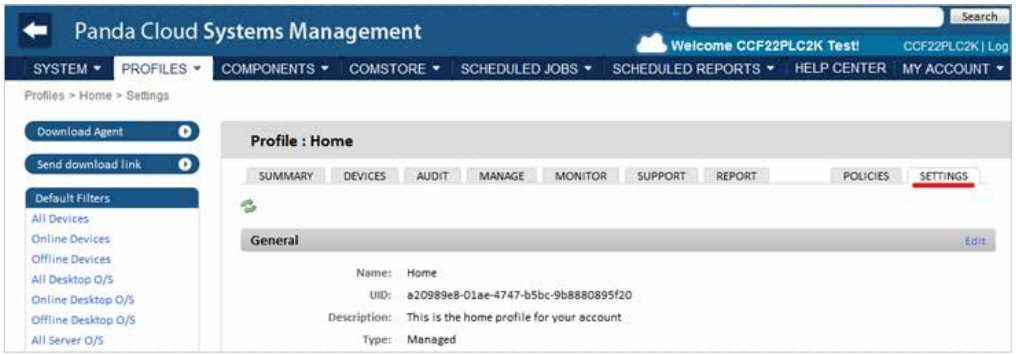
System Level tiene la capacidad de realizar acciones de forma global. Así, es posible obtener listados con el estado de todos los dispositivos administrados, informes consolidados relativos al sistema y acciones sobre todos o parte de los dispositivos registrados.

PROFILE LEVEL

¿Qué es?

Profile Level es la entidad de agrupación inmediatamente inferior a System. Es una agrupación lógica que contiene los dispositivos que pertenecen a una misma cuenta de cliente o delegación.

La lista de Profiles es accesible desde el Menú General, Profiles.
Cada Profile lleva asociado una serie de configuraciones accesibles desde la Barra de Pestañas, Settings en la **Consola PCSM**, que a su vez son empaquetadas con el **Agente PCSM**.

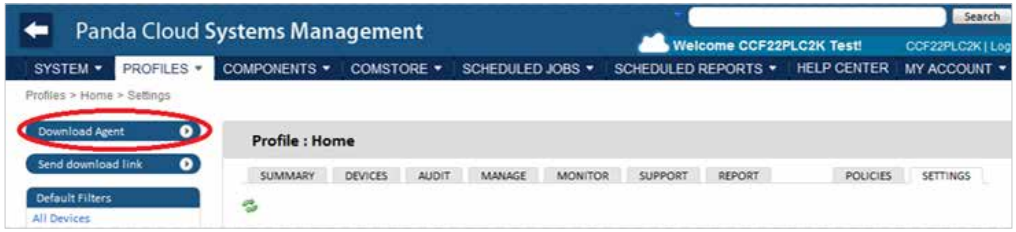


Las opciones de configuración se pueden dividir en varios grupos:

- **Identificación del Profile**
  Se trata de información que permite identificar al Profile entre el resto de Profiles generados y que se utiliza en filtros o búsquedas. Los campos que podemos configurar son los siguientes:
  - **General**: Nombre y descripción del Profile.
  - **Variables**: variables de entorno que heredarán los dispositivos que pertenecen al Profile y que podrán ser invocadas más tarde desde scripts o componentes desarrollados por el administrador. En el capítulo 10 se describe la creación y distribución de componentes.
  - **Custom Labels**: cinco campos con información a discreción del administrador.
- **Información de contacto**
  Son las cuentas de correo que el **Panda Cloud Systems Management** utilizará para contactar con los administradores del servicio. Generalmente son utilizadas para el envío de informes o de alertas.
- **Mail Recipients**
- **Caché local**
  Se indica en este campo el dispositivo que servirá de cache en la LAN del cliente para acelerar la descarga de software, los parches o los scripts que más tarde se distribuirán entre los dispositivos vecinos. Este método permite reducir el consumo de ancho de banda al evitar que los dispositivos que pertenezcan a una misma red tengan que salir a Internet de forma independiente para descargar estos elementos.
- **Información de Login**
  La ejecución de scripts en el dispositivo del usuario hereda los permisos asociados a la cuenta Localhost, pero si el Profile necesita ejecutar scripts con el comando Run As podemos indicar aquí la información de Login y Password.

✔ **Información de consumo**
Podemos asociar información de consumo eléctrico a cada rol de dispositivo para que el **Servidor PCSM** realice un recuento de consumos global y pueda contrastarlo frente a variantes en la configuración de ahorro de energía, a través de System Policies o Profile Policies, explicadas más adelante.

Aparte de la información indicada, el **Agente PCSM** lleva incrustada la pertenencia al Profile que lo generó, ya que es directamente descargable desde la misma pantalla de administración del Profile.



Cuando el Agente PCSM se instale en los dispositivos del cliente éstos se añadirán automáticamente al Profile correcto en la Consola PCSM.

Ámbito
Los procedimientos desencadenados en Profile Level podrán afectar a todos los dispositivos que pertenecen a ese Profile, si bien algunas acciones podrán ser limitadas a un subconjunto de dispositivos mediante filtros y grupos, descritos en el capítulo 5.

A diferencia de System Level que es único, el administrador podrá crear tantas agrupaciones Profile como considere oportuno.

Pertenencia
La pertenencia de un dispositivo administrado a un Profile u otro queda determinada por la instalación del Agente PCSM.

Descargue el **Agente PCSM** desde la página del Profile elegido de forma que al instalarse en el dispositivo del usuario éste se agregará de forma automática al Profile en cuestión en la **Consola PCSM.**

Es posible mover dispositivos de un Profile a otro desde la **Consola PCSM** una vez instalado el **Agente PCSM** en el dispositivo del usuario.

Para minimizar las tareas en la fase de distribución se recomienda primero crear el Profile y después descargar desde éste el **Agente PCSM**, de forma que la pertenencia de los dispositivos administrados al Profile creado sea automática.

Funcionalidad
Profile Level tiene la capacidad de realizar acciones sobre todos los dispositivos que lo forman. De esta forma es posible obtener listados con el estado de dispositivos, informes consolidados y acciones sobre todos o sobre parte de los dispositivos que forman el Profile.

DEVICE LEVEL
¿Qué es?
Es la representación lógica en la **Consola PCSM** de un único dispositivo con un **Agente PCSM** ya instalado y reportando información al **Servidor PCSM**. La creación de Devices en la **Consola PCSM** es automática ya que se añaden según se vayan instalando **Agentes** en los dispositivos del cliente.

Ámbito
Todas las acciones realizadas en este nivel afectan únicamente al dispositivo seleccionado.

Funcionalidad
Device Level tiene la capacidad de realizar acciones sobre un dispositivo particular. De esta forma es posible obtener listados lo más detallados posible del dispositivo e informes y acciones.

A lo largo de esta guía se distingue entre "Device" y "dispositivo". "Device" se utiliza cuando se refiere a la entidad que representa al dispositivo en la **Consola PCSM**, es decir, el "Device Level", mientras que "dispositivo" es el equipo informático físico administrado.

04. ELEMENTOS BÁSICOS DE LA CONSOLA PCSM

La Consola PCSM queda estructurada de una forma intuitiva y visual, de forma que la mayor parte de los recursos de administración queden a un clic de distancia, evitando así el exceso de checkboxs y configuraciones innecesarias.

El objetivo es una **Consola PCSM** lo más limpia posible, rápida de utilizar y cómoda, que evite en lo posible las recargas de página completas y que ofrezca una curva de aprendizaje muy poco pronunciada y corta para el departamento de IT; de esta manera se podrá entregar valor al cliente desde el primer momento.

Los elementos básicos de la **Consola PCSM** a los que se hace referencia a lo largo de esta guía son.

MENÚ GENERAL

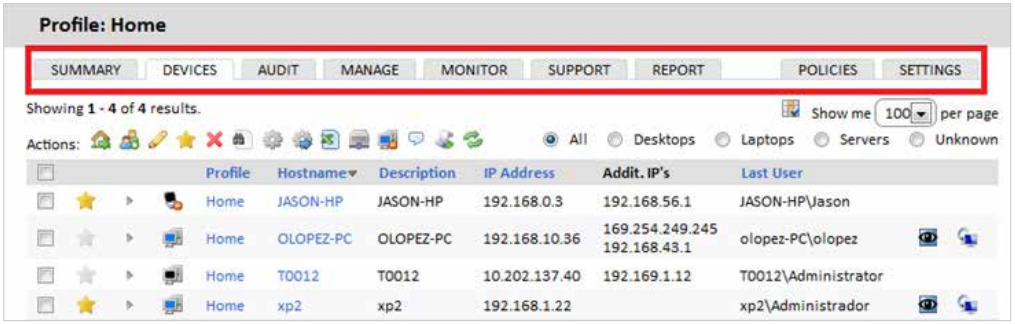
Es el menú accesible desde cualquier punto de la **Consola PCSM**. Consta de ocho entradas.

Menú	Descripción
System	Acceso al System Level.
Profiles	Acceso al Profile Level.
Components	Acceso a los componentes descargados y accesibles por el administrador.
ComStore	Repositorio de componentes creados por Panda Security que extienden la funcionalidad de **PCSM**.
Scheduled Jobs	Listado de jobs activos y terminados.
Scheduled reports	Listado de informes configurados y ya generados.
Help Center	Centro de ayuda con links a recursos de Panda.
Account	Acceso a los datos de la cuenta de administración principal así como a los recursos para crear nuevos roles y usuarios. Más información en el capitulo 14.

BARRA DE PESTAÑAS / BARRA DE LISTADOS

La Barra de Pestañas o también Barra de Listados permite el acceso a las herramientas de la **Consola PCSM** orientadas fundamentalmente a la generación y presentación de listados consolidados en pantalla, con información de estado de los dispositivos que pertenecen al nivel accedido, aunque también permite la creación y visualización de configuraciones.

Esta barra varía ligeramente si es accedida desde el Profile Level, System Level o Device Level para un dispositivo concreto, ya que el ámbito de administración es diferente.



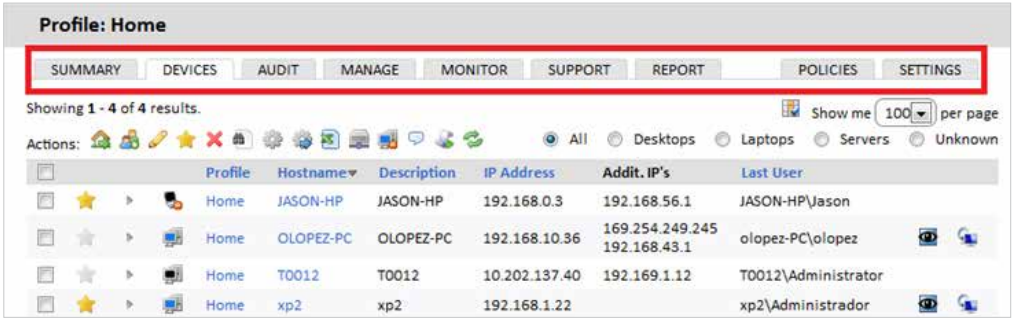
Pestaña	Accesible desde	Descripción
Summary	Profile, Device	Información de estado.
Dashboard	System	Panel de control general.
Devices	Profile	**Listado de dispositivos** accesibles con información asociada.
Audit	System, Profile, Device	**Listado del inventariado** del hardware, software y licencias.
Manage	System, Profile, Device	**Listado de parches** aplicados y pendientes de aplicar.
Monitor	System, Profile, Device	**Listado de alertas** generadas por monitores o jobs terminados.
Support	System, Profile, Device	**Listado de tickets** generados
Report	System, Profile, Device	**Listado y generación** bajo demanda de Infomes.
Policies	System, Profile, Device	**Listado y generación** de Políticas, explicadas más adelante.
Settings	Profile	**Configuración** asociada al Profile.
Suspended devices	System	**Listado** de Devices desinstalados.

El ámbito de la Barra de Pestañas se refiere al nivel actual. De este modo, si accedemos a la Barra de Pestañas en el System Level nos mostrará la información de todos los Devices, si accedemos en el Profile Level mostrará información consolidada de los Devices que participan del Profile. Si accedemos en el Device Level, solo se mostrará información de ese Device en particular.

BARRA DE ICONOS / BARRA DE ACCIONES

La Barra de Iconos o Barra de Acciones permite el acceso a las acciones orientadas a modificar el estado de los dispositivos. Esta barra no existe en el Menú General, System de forma directa y varía ligeramente si es accedida desde el Menú General, Profile o desde un Device particular ya que el ámbito de administración es diferente.

El ámbito de acción de la Barra de Iconos será el formado por la selección manual de Devices que hayamos marcado dentro de un Profile.



Icono	Accesible desde	Descripción
Move Device to	Profile, Device	**Mueve el o los Devices** seleccionados a otro Profile.
Add Device to	Profile, Device	**Añade el o los Devices** seleccionados a un grupo.
Edit	Profile	**Añade notas** y campos custom a los Devices seleccionados que podrán ser utilizados por los filtros.
Toggle	Profile	Marca como favorito Devices para su acceso rápido desde Summary / Dashboard.
Delete	Profile, Device	**Borra un Device de un Profile**. El Device dejará de ser administrado, el **Agente PCSM** se desinstalará y el dispositivo se añadirá a la Pestaña Suspended Devices del Menú General, System

Continua

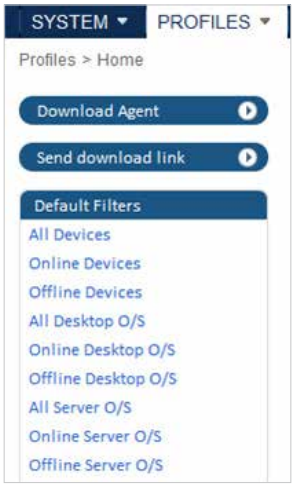
Icono	Accesible desde	Descripción
Request audit	Profile, Device	**Fuerza el lanzamiento** de un inventariado (el inventariado es una tarea automática que se realiza cada 24 horas).
Schedule Job	Profile, Device	**Crea un trabajo programado** para una fecha posterior.
Run Job	Profile, Device	**Ejecuta en el momento un trabajo** ya creado.
Download	Profile	**Descarga del listado de dispositivos** del Profile.
Add/Remove Cache	Profile, Device	**Marca al dispositivo como Cache** de la red.
Turn Privacy	Profile, Device	**Impide el acceso remoto** por parte del administrador a los dispositivos si no es con la aprobación manual del usuario
Send a message	Profile, Device	**Envía un mensaje** a los dispositivos seleccionados.
Schedule reports	Profile	**Programa un informe** para una fecha posterior.
Refresh	Profile, Device	Refresca los datos en pantalla.
Initiate	Device	**Inicia la instalación de los Agentes** en los dispositivos pertenecientes a la misma red.
QR Code	Device	Código QR asociado al dispositivo para su inventariado en papel.

Si quiere realizar acciones en el System Level tendrá que crear un filtro o grupo ya que el System Level no muestra la Barra de Iconos por defecto.

PANEL DE GRUPOS Y FILTROS

En la parte izquierda de la Consola PCSM se encuentran tres paneles con grupos de diversos tipos:

- **Default Filters**: filtros generados por el sistema automáticamente.
- **Profile Filters / System Filters**: filtros de dispositivos creados por el administrador en el Profile Level o System Level respectivamente.
- **Profile Device Groups / System Device Groups**: grupos de dispositivos creados por el administrador en el Profile Level o System Level respectivamente.
- **System Profile Groups**: disponibles únicamente en el System Level, son agrupaciones de varios Profiles.

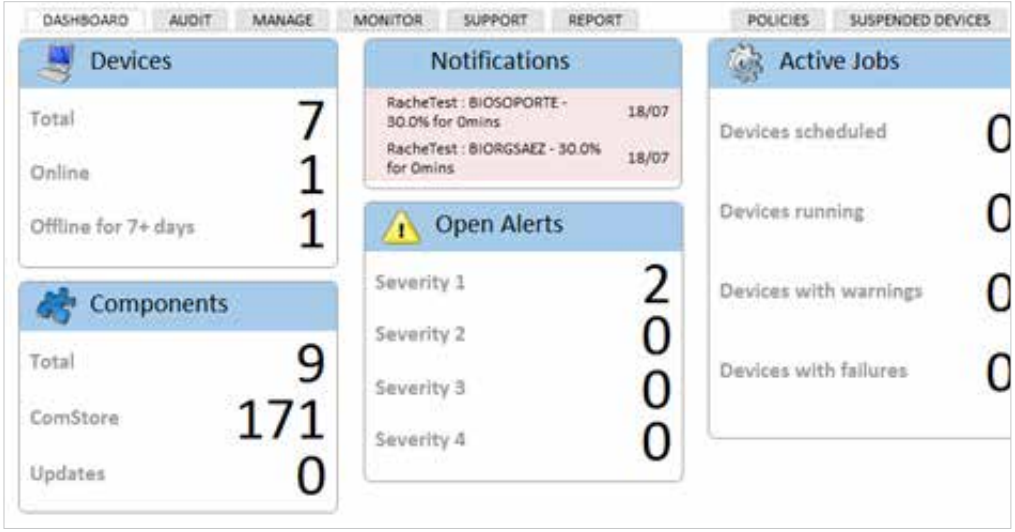


PANELES DE CONTROL

Los paneles de control (dashboards) reflejan el estado de un conjunto de dispositivos. Existen cuatro tipos de paneles de control.

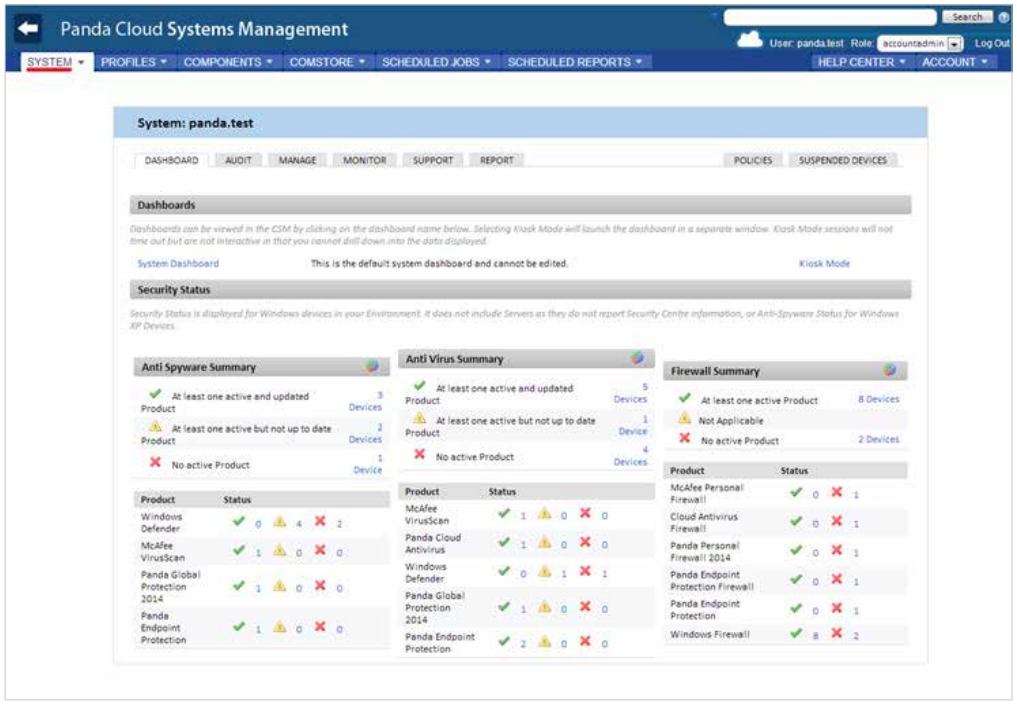
System Dashboard

Accesible desde el Menú General, System haciendo clic en System Dashboard.



Security Status

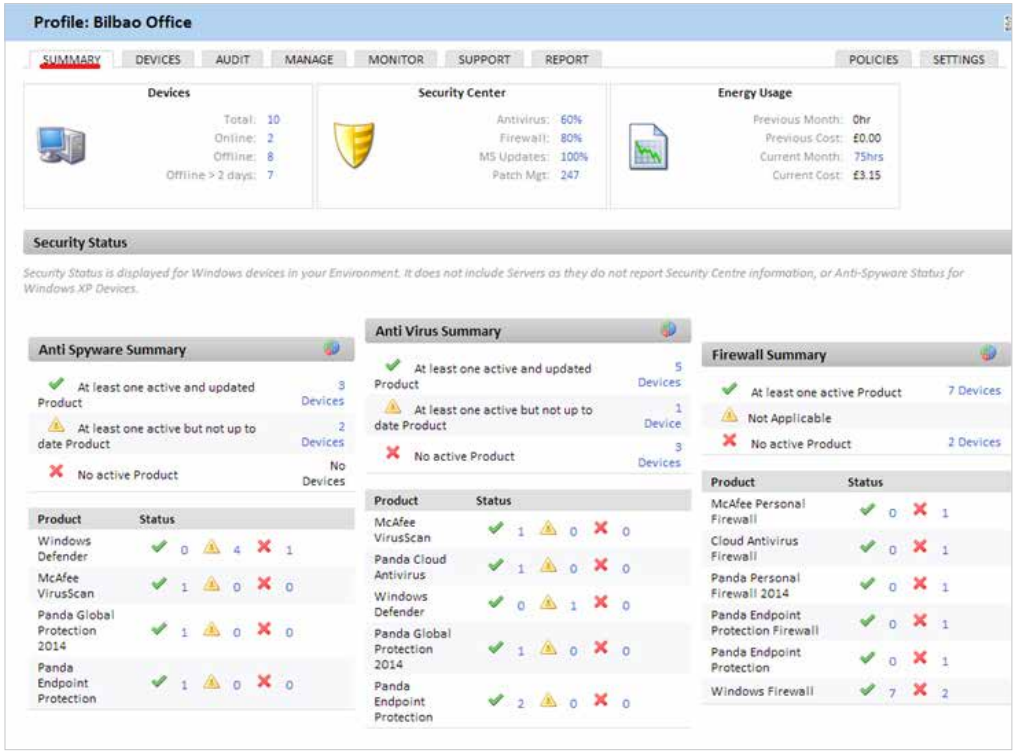
Accesible desde el Menú General, System, refleja el estado de la seguridad de los dispositivos gestionados.



Reúne información general del estado del parque de dispositivos: Notificaciones, jobs, Alertas, etc.

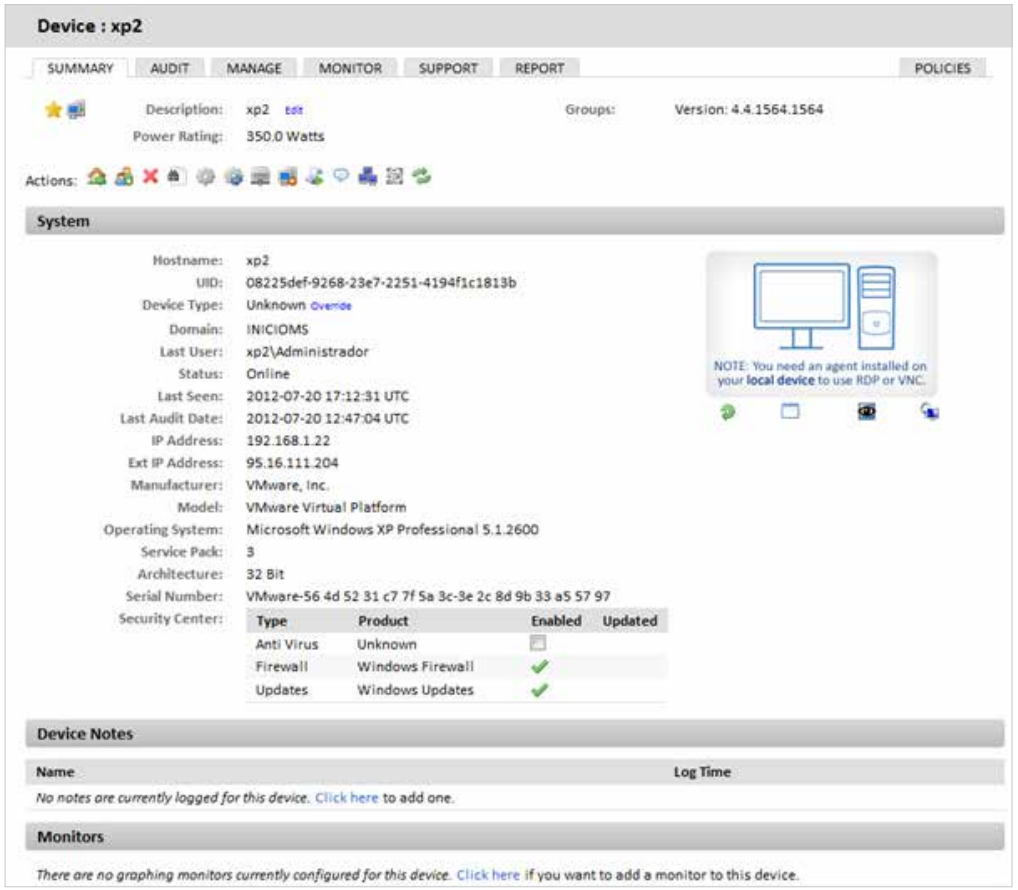
Summary (Profile)

Accesible desde el Menú General, Profile. Refleja el estado de todos los dispositivos que pertenecen al Profile seleccionado. Habrá un Panel de control Summary por cada Profile creado.



Summary (Device)

Accesible desde un Device. Refleja el estado del dispositivo concreto. Habrá tantos como dispositivos administrados.



05. FILTROS Y GRUPOS

¿QUÉ SON LOS GRUPOS Y FILTROS?

Los grupos y filtros son recursos destinados a generar agrupaciones de dispositivos similares al Profile pero de una forma más ágil y dinámica. Así, mientras en la creación de un Profile se consideran aspectos de los dispositivos de marcado aspecto estático como la pertenencia a una cuenta de cliente concreta, los grupos y filtros están diseñados para ser modificados con agilidad atendiendo a características o criterios temporales de los dispositivos.

TIPOS DE GRUPOS Y FILTROS

Se soportan varios tipos de grupos / filtros:

- **Profile Device Groups / Profile Filters**: creados dentro de un Profile determinado, solo pueden contener dispositivos que pertenecen al Profile seleccionado.
- **System Device Groups / System Filters**: creados en el System Level pueden contener dispositivos que pertenecen a uno, varios o todos los Profiles
- **System Profile Groups**: creados en el System Level son agrupaciones de Profiles.

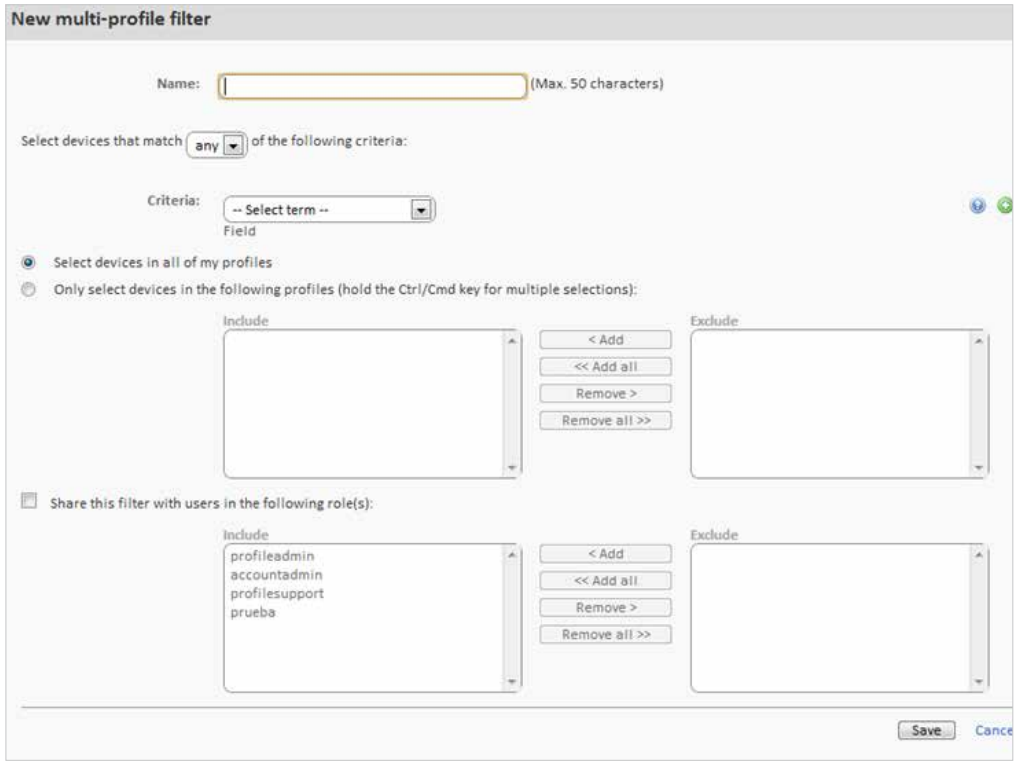
Los filtros y los grupos pueden ser agrupaciones de dispositivos inter - Profile: dependiendo de donde se generen pueden abarcar dispositivos de uno o varios Profiles.

GRUPOS

Los grupos son agrupaciones de dispositivos estáticas. La pertenencia de un dispositivo a un grupo es manual por asignación directa.

FILTRO

Los filtros son agrupaciones de dispositivos dinámicas. La pertenencia de un dispositivo a un filtro es automática de forma indirecta, según se hayan configurado sus condiciones de pertenencia. Las condiciones de pertenencia de un filtro pueden ser una o varias y están relacionadas entre sí por operadores lógicos (AND / OR).



A continuación se indican los pasos para construir un filtro.

- **Indicar el nombre del filtro**. Se recomienda que sea descriptivo indicando las características comunes de los dispositivos agrupados (p. ej. "Servidores Microsoft Exchange", "Workstations con poco espacio de disco").
- Si hay múltiples condiciones determinar la **operación lógica** que se aplicará entre ellas:
  - **Any**: cualquier dispositivo que cumpla al menos una condición entrará a formar parte del filtro.
  - **All**: solo los dispositivos que cumplan todas las condiciones entrarán a formar parte del filtro.
- **Criteria**: cada línea de condiciones consta de varios campos que la describen, según el tipo:
  - **Field**: es el campo principal que indica que característica del dispositivo se tomará para incluirlo como parte del filtro. Los principales campos Criteria están enumerados y clasificados más abajo.
  - **Condition**: establece el modo de comparación del campo Field con lo que el administrador establezca.
  - **Search Term**: campo que describe contenido del campo Field. Dependiendo del tipo del campo Condition el campo Search Term cambiará para reflejar intervalos de fechas, literales, etc.

A continuación se indican los distintos valores disponibles para cada línea de condición Criteria.

Campo	Condición	Término de búsqueda
String	Vacío – No vacío Contiene – No contiene Comienza – No comienza con Termina – No Termina con	Cadena de caracteres. Utilizar % como comodín para machear cualquier numero de caracteres.
Integer	Mayor – Mayor o igual que Menor – Menor o igual que Entre inclusivo, Entre exclusivo	Numérico.
Binary	True / False	
Date	Antes – Después de Más viejo de 30/60/90 días	Intervalo de fechas.

- ✔ **Añadir** varias líneas de tipo Criteria con los iconos + y – de la derecha.
- ✔ **Seleccionados el ámbito del filtro**:
  - ✔ Todos los Devices en todos los Profiles.
  - ✔ Solo los Devices de los Profiles indicados.
- ✔ Seleccionamos usuarios de la **Consola PCSM** que tendrán acceso al filtro.

Las características descritas en el campo Field se puede agrupar de la siguiente manera según su función descriptora del dispositivo:

Estado del dispositivo	Status – Online/Offline	Dispositivo encendido o apagado.
	Status suspended	Equipos suspendidos.
	Antivirus On/Off	
	Firewall On/Off	
	Free disk capacity	Detecta dispositivos con espacio de almacenamiento libre bajo.
	Windows updates On/OFF	Equipos suspendidos.
Rol del dispositivo	Discrimina los dispositivos por su función principal.	
	Device Type: Server, Workstation, Smartphone, LapTop	
	Operating System	Permite discriminar sistemas operativos de servidor o de cliente.
	Arquitecture	32 o 64 bits.

Continua

Versiones de software		
	Service Pack	Versión de SP instalado
	Software Package	Software instalado
	Software versión	
Hardware	Información del Vendor, modelo, revisión, etc.	
	CPU	
	BIOS Name/Release/ versión	
	Display Adapter	
	Manufacturer	
	Memory	
	Model	
	Monitor	
	Motherboard	
	Network Adapter	
Id del dispositivo	Información que identifica y describe al dispositivo.	
	Description	Descripción libre
	Profile Description	

Continua

Id del dispositivo	Información que identifica y describe al dispositivo.	
	Profile name	
	Domain	
	IP Address	
	MAC Address	
	Serial number	
	Hostname	
Otros estados		
	Favourite	Para el acceso rápido desde el dashboard.
	Last seend date	
	Last audit	
	Last user	

06. CÓMO ORDENAR LOS DISPOSITIVOS ADMINISTRADOS DE FORMA EFICIENTE

La distribución en la **Consola PCSM** de los dispositivos administrados en un MSP con múltiples cuentas de cliente o en un departamento de IT con varias delegaciones, afecta a la eficiencia de forma notable, ya que muchos procedimientos y acciones pueden configurarse para ser ejecutadas sobre gran cantidad de dispositivos siguiendo una correcta combinación de Profiles, grupos y filtros.

DIFERENCIAS ENTRE PROFILES, GRUPOS Y FILTROS

A continuación se describen las ventajas y limitaciones de las tres formas de agrupación soportadas.

Profiles

- **Ventajas**
  - Asocian una misma configuración de salida a Internet a todos los dispostivos: ahorra la configuración manual dispositivo por dispositivo en local.
  - Asocian información de contacto vía email para el envío de Informes, Alertas, Tickets etc.
  - Tienen acceso a la Barra de Pestañas y a la Barra de Iconos con lo que permiten la ejecución de Acciones y la visualización de Listados e Informes consolidados, abarcando a todos los Devices del Profile de forma cómoda y rápida.

- **Limitaciones**
  - Un Device concreto solo puede pertenecer a un único Profile.
  - No es posible generar Profiles dentro de Profiles.

Grupos y filtros

- **Ventajas**
  - Los groups / filters permiten crear subconjuntos de dispositivos dentro de un único Profile o incluso de diferentes.
  - Un dispositivo puede pertenecer a varios groups / filters.
- **Inconvenientes**
  - Los groups / filters tienen funcionalidad limitada ya que se pierde el acceso a la Barra de Pestañas con lo que no es posible la generación de Listados consolidados.
  - El acceso a los Informes es limitado, solo se generan informes que contienen información de un único dispositivo.

> Los groups / filters son a los efectos Profiles dentro de Profiles (tantos como queramos) pero con acceso limitado a la funcionalidad de Informes consolidados y a la Barra de Pestañas.

ENFOQUE GENERAL Y ESTRUCTURA DE ORDENACIÓN DE DISPOSITIVOS

Se aplican las siguientes normas de carácter general:

- **Agrupar los dispositivos en Profiles para separar los dispositivos de Cuentas de cliente distintas.**
  Los Profiles no imponen ningún tipo de limitación en la generación de Informes o Listados consolidados y permiten aplicar configuraciones a todos los Devices de un Profile.
- **Crear Profile Device Groups para agrupar dispositivos de hardware / software / configuración / uso similar.**
  Por ejemplo configurar Profile Device Groups para segregar dispositivos por departamentos dentro de una misma cuenta de cliente con necesidades similares (software utilizado, requisitos generales, acceso a impresoras etc) o con roles muy diferenciados (Servidores vs Workstations).
- **Crear Profile Filters para buscar equipos con estados comunes dentro de un Profile.**
  Utilizar filtros para establecer búsquedas rápidas y automáticas que permitan localizar condiciones anómalas o que caigan fuera de umbrales predeterminados (poco disco libre, poca memoria física instalada, software no permitido etc) de forma proactiva, o para buscar equipos con características concretas.

> No deberíamos utilizar de forma general filtros para agrupaciones de carácter estático.

- **Crear System Profile Groups para agrupar Profiles.**
  En el caso de que existan cuentas de cliente o delegaciones muy similares en las características y variedad de dispositivos es posible agruparlas en un mismo System Profile Group para así acelerar su gestión.
- **Asociar Account Groups y Filters a perfiles técnicos.**
  Si el tamaño del MSP es medio-alto llegará un momento en que tenderá a la especialización de su personal técnico. De esta forma habrá técnicos que solo administren cierto tipo de dispositivos concretos, como servidores de correo Exchange o Workstations Windows XP por ejemplo. Un grupo o filtro de tipo System ayuda a localizar y a agrupar estos equipos sin tener que ir Profile por Profile en su búsqueda. Para completar el escenario descrito es indicado crear y configurar roles y nuevas cuentas de usuario según se describe en el capítulo 14.

07. LOS 8 PRIMEROS PASOS PARA COMENZAR A USAR PCSM

CREACIÓN Y CONFIGURACIÓN DEL PRIMER PROFILE

En primer lugar se debe de determinar si crear un nuevo Profile o reutilizar uno ya en uso, dependiendo de los criterios de ordenación que estemos utilizando. De forma general, una nueva cuenta de cliente se corresponderá con un Profile nuevo.

Rellenamos la información necesaria teniendo en cuenta que el campo descripción podrá ser utilizado posteriormente por filtros que demos de alta y que referencien al contenido de este campo.

Si los dispositivos del Profile requieren información adicional de Proxy HTTP para acceder a Internet, esta información podrá ser suministrada aquí o más tarde.

Una vez creado el Profile se recomienda configurarlo a través de la pestaña Settings. Esta configuración será incorporada en el **Agente PCSM** a instalar en cada dispositivo administrable.

DEPLOY DEL AGENTE PCSM

El **Agente PCSM** que instalaremos en los dispositivos del cliente requiere cierta información básica para poder funcionar:

- ✔ El Profile al que va a pertenecer.
- ✔ La información mínima para poder salir a Internet y conectarse con el Servidor PCSM.

El Profile al que pertenecerá el **Agente PCSM** queda automáticamente establecido si iniciamos la descarga o envío desde el propio Profile.

La información de salida a Internet fue indicada en el paso anterior al crear el Profile o en la Barra de Pestañas, Settings de forma que el **Agente PCSM** que descarguemos ya contendrá dicha información.

La descarga del **Agente PCSM** se puede realizar de dos maneras:

- ✔ Envío del **Agente PCSM** descargado (correo, deploy con Active Directory, etc.)
- ✔ Envío por correo de la URL de descarga.

La instalación del **Agente PCSM** en redes con muchos dispositivos puede ser larga y tediosa si tenemos que realizar el envío a cada dispositivo de forma independiente. La forma más simple de realizar un deploy masivo es:

- ✔ Envío del Agente PCSM al primer dispositivo de la red.

Normalmente la instalación del **Agente PCSM** únicamente requiere un doble clic en el paquete descargado, sin necesidad de confirmaciones, completamente "silent". Una vez instalado el **Agente PCSM** se conectara al **Servidor PCSM** y aparecerá en el listado de dispositivos administrados en el Profile seleccionado.

- ✔ Deploy automático al resto de dispositivos de la red.

Seleccionando el Dispositivo con el primer **Agente PCSM** instalado se podrá iniciar una instalación a todo el segmento de red.

COMPROBACIÓN DEL LISTADO DE DISPOSITIVOS DEL PROFILE Y FILTRADO BÁSICO

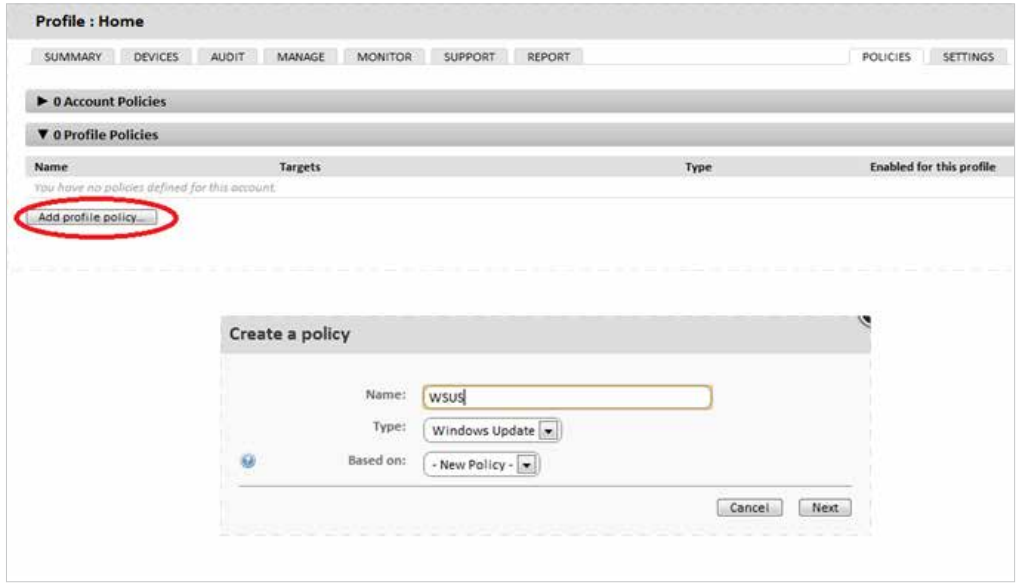
Podemos marcar los equipos como favoritos para acceder a ellos de forma rápida más adelante, ordenar los listados, filtrarlos de forma rápida por el rol del dispositivo y dimensionar el listado para mostrar más o menos elementos.

INVENTARIADO DE HARDWARE, SOFTWARE Y LICENCIAS

En la Barra de Pestañas, Audit tenemos toda la información de inventariado de los dispositivos que pertenecen al Profile o, si es accedida desde el Device Level nos mostrará la información relativa al dispositivo de forma más detallada.

PATCH MANAGEMENT

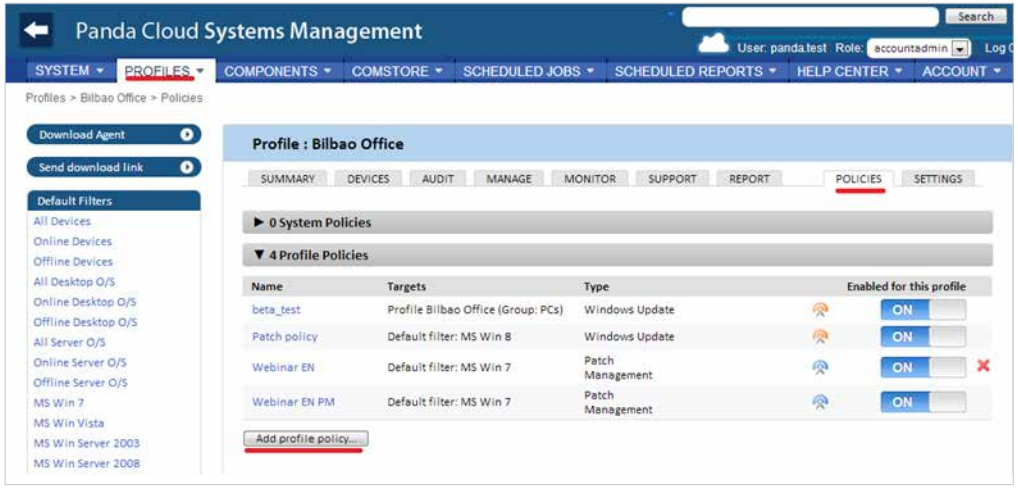
Apruebe los parches que no han sido instalados en los dispositivos administrados o ejecute un rollback de aquellos que quiera desinstalar en la Barra de Pestañas, Manage. Configure cuándo se aplicarán los parches en los dispositivos del Profile, el comportamiento a seguir una vez aplicados y otros parámetros creando una policy de Windows Update o Patch Management desde la Barra de Pestañas, Policies en el Profile. Para más información sobre Patch Management consultar el capítulo 13. Para más información sobre la creación de Policies consultar el capítulo 8.



CREACIÓN DE MONITORES

Distribuya mecanismos de monitorización en los dispositivos de la red.

Desde el Menú General, System o desde un Profile concreto en la Barra de Pestañas, Policies hacemos click en Add System/Profile Policy.



En el tipo de policy elegimos monitor.

Añadimos un target (uno o varios grupos o filtros) y un monitor. Al añadir un monitor se mostrará un wizard de 4 pasos donde especificaremos la configuración necesaria.

Más información sobre monitores en el capítulo 9.

COMSTORE

Extienda la funcionalidad de **PCSM** e instale software de terceros de forma centralizada con los componentes publicados en la ComStore.

Los componentes directamente utilizables por el partner / administrador de IT deberán de ser descargados desde la ComStore.

Bajo "My Components" aparecen los componentes ya descargados y utilizables.

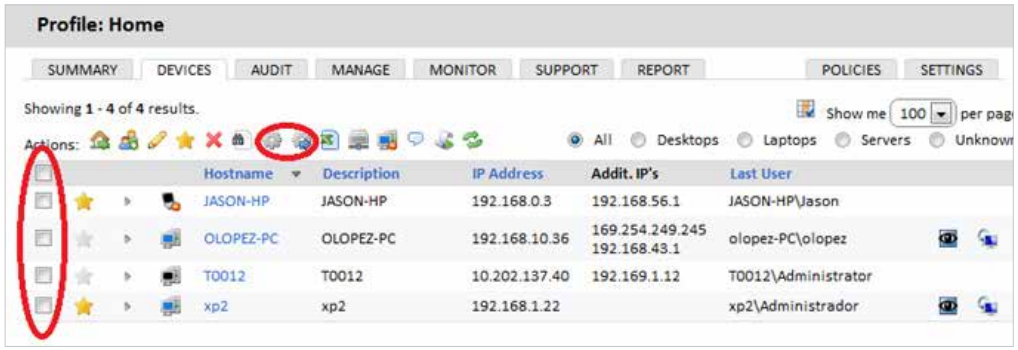
Bajo "ComStore" aparecen los componentes accesibles para descarga de la ComStore.

Para descargar un componente seleccionar uno y pinchar en "Buy". En ese momento se incorporará al apartado My Components.

Todos los componentes de la ComStore son gratuitos.

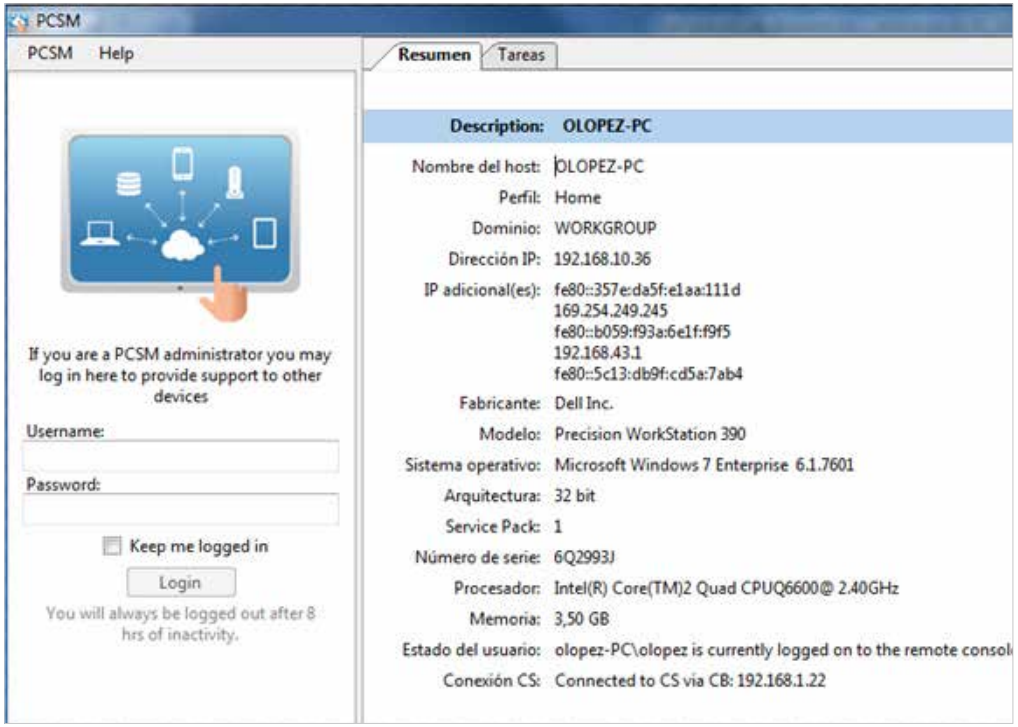
Dependiendo del tipo de componente podrá ser ejecutado como una tarea (job) o como respuesta a una alerta generada por un monitor.

En la Barra de Pestañas, Devices dentro del Profile seleccionamos los dispositivos a aplicar el componente y elegimos entre programar un trabajo (Schedule a job) o ejecutarlo de forma inmediata (Run a quick Job).

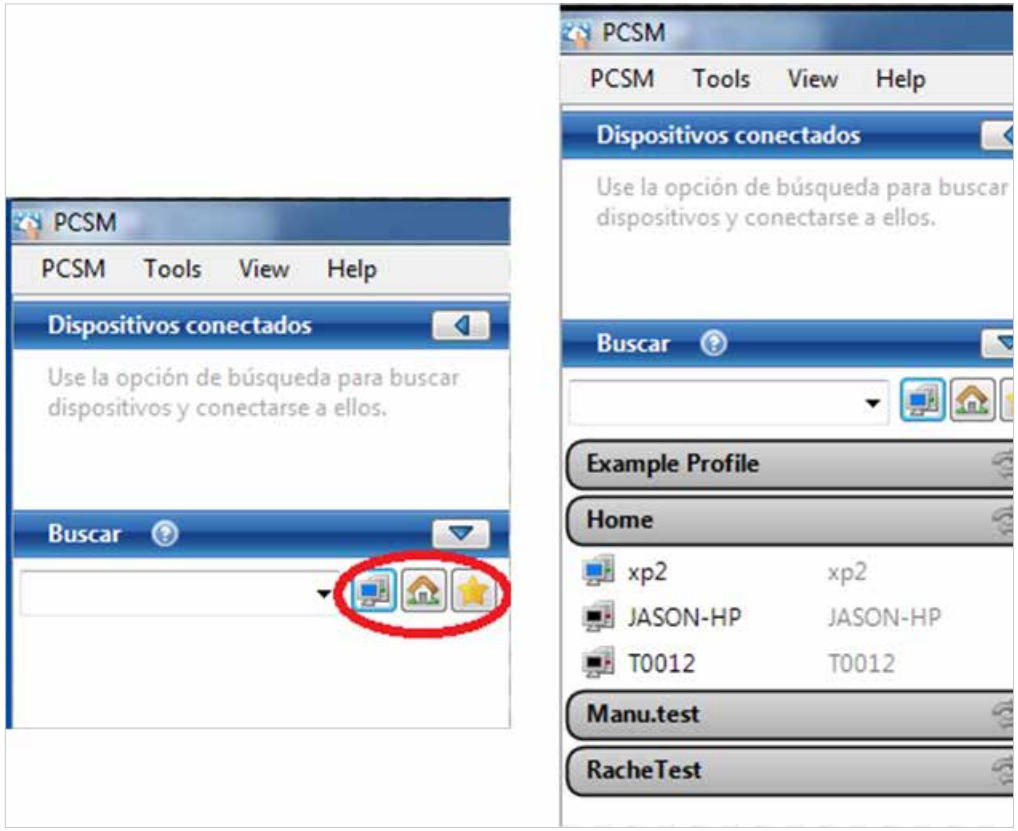


ACCEDA A LOS RECURSOS DE LOS DISPOSITIVOS REMOTOS ADMINISTRADOS

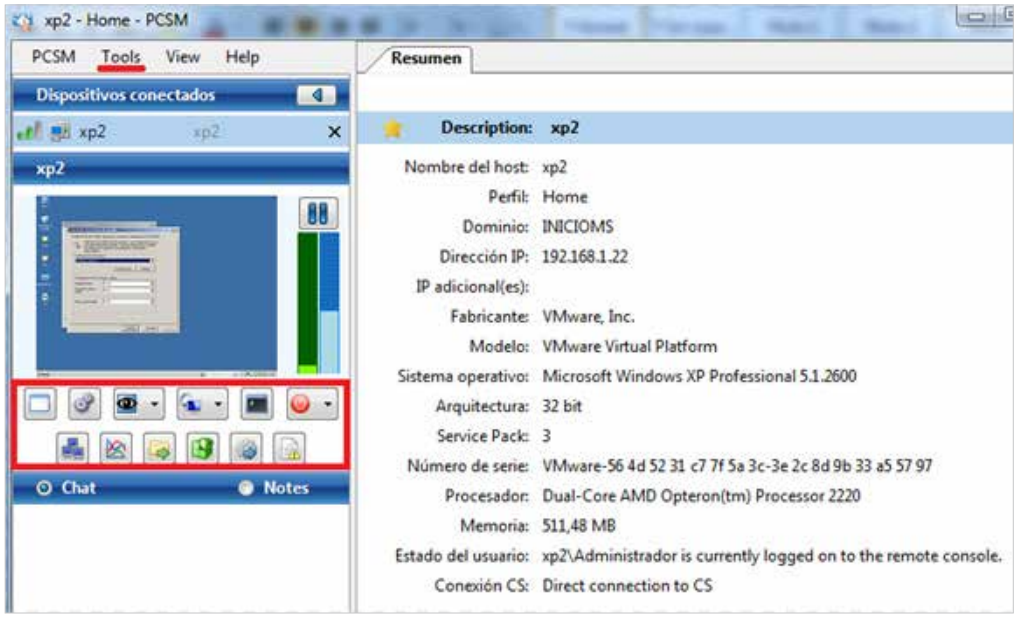
A pesar de que muchas operaciones cotidianas pueden realizarse directamente desde la **Consola PCSM** puede ser necesario acceder directamente al dispositivo mediante el **Agente PCSM**. Para ello es necesaria su instalación en el dispositivo del técnico que dará el soporte remoto y hacer login con su usuario y contraseña.



Iniciada la sesión buscamos el dispositivo a administrar bien por su nombre, desplegando los Profiles a los que tiene acceso el técnico con las credenciales suministradas o listando los equipos marcados como favoritos.



Una vez localizado el dispositivo quedarán accesibles todas las opciones de control remoto y acceso remoto tanto a través de los iconos como de los menús.



Las opciones disponibles que no impiden al usuario seguir trabajando con el dispositivo son:

- ✔ **Captura de pantalla remota**: visualización rápida de mensajes de error.
- ✔ **Pestaña de Servicios de Windows**: acceso a parada arranque y reinicio de servicios sin necesidad de acceder al escritorio remoto.
- ✔ **Sesión de pantalla compartida**: escritorio remoto compartido. El usuario ve lo que el técnico está haciendo en su dispositivo.
- ✔ **Shell de comandos**: línea de comandos DOS remota.
- ✔ **Implementación del agente**: lanzamiento del deploy del Agente PCSM en la LAN.
- ✔ **Administrador de tareas**: acceso al administrador de tareas sin necesidad de acceder al escritorio remoto.
- ✔ **Transferencia de archivos**: envío y recepción de ficheros.
- ✔ **Editor del registro**: acceso a la herramienta de Regedit sin necesidad de acceder al escritorio remoto.

- **Trabajos rápidos**: lanzamiento de jobs.
- **Visor de eventos**: acceso al visor de sucesos sin necesidad de acceder al escritorio remoto.
- **Wake Up**: permite que un dispositivo en funcionamiento envíe al resto de dispositivos dentro del mismo segmento de LAN un "magic packet" para encenderlos remotamente. Las opciones que interrumpen el trabajo del usuario con el dispositivo son:
- **RDP de Windows**: acceso al escritorio remoto por RDP, lo que implica el cierre de la sesión del usuario.
- **ShutDown / Reboot**: reinicio de la máquina.

08. POLÍTICAS / POLICIES

¿QUE SON LAS POLICIES?

Cualquier configuración o comportamiento específico que se repita a intervalos regulares a lo largo del tiempo, en uno o varios dispositivos administrados por **PCSM** se implementa empujando una policy a cada **Agente PCSM** instalado. Las Policies son contenedores de configuraciones formadas por:

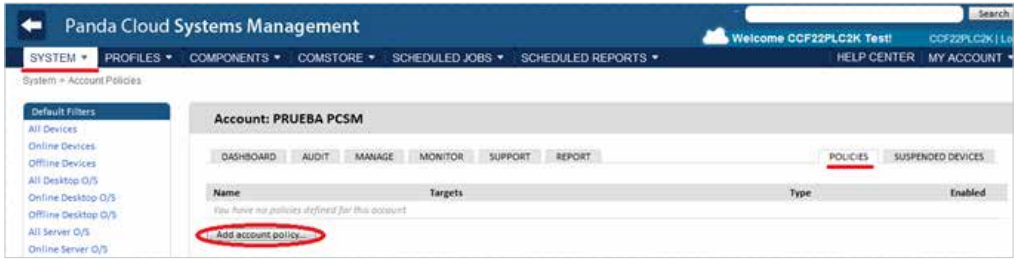
- Targets: agrupaciones de dispositivos que se verán afectados por la policy.
- Servicios: según el Tipo de la policy el **Agente PCSM** realizará una serie de acciones concretas en cada dispositivo.

Las Políticas pueden crearse en los tres niveles disponibles dependiendo del número de dispositivos y su pertenencia a un mismo cliente o a varios:

- System Policy: define un comportamiento aplicable a System Profile Groups, System Filters o System Device Groups.
- Profile Policy: define un comportamiento aplicable a Profile Groups o Profile Filters.
- Device Policy: define un comportamiento aplicable a un dispositivo concreto.

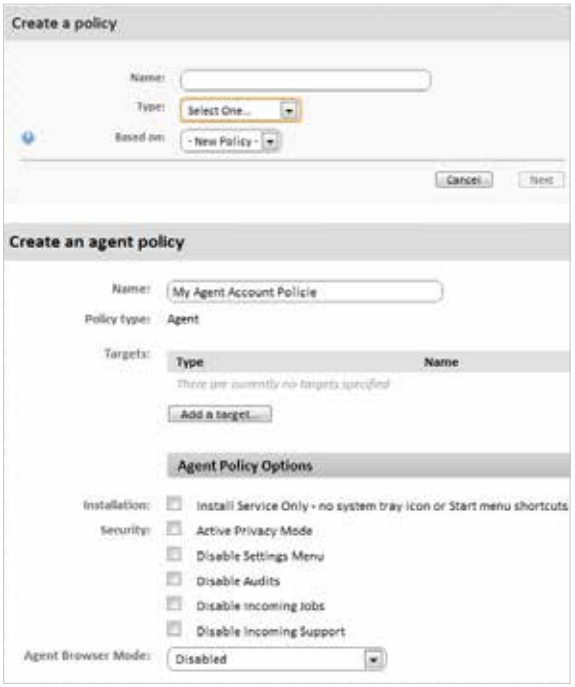
¿CÓMO DEFINO UNA SYSTEM POLICY?

Desde el Menú General, System clicando en la Barra de Pestañas, Policies.



Se mostrará una ventana donde indicamos el nombre de la policy, su Tipo y si está basada en otra policy creada anteriormente, para agilizar su generación.

La siguiente ventana pide todos los datos necesarios para configurar la policy. Según el tipo de policy que hayamos elegido esta ventana pedirá unos datos u otros.

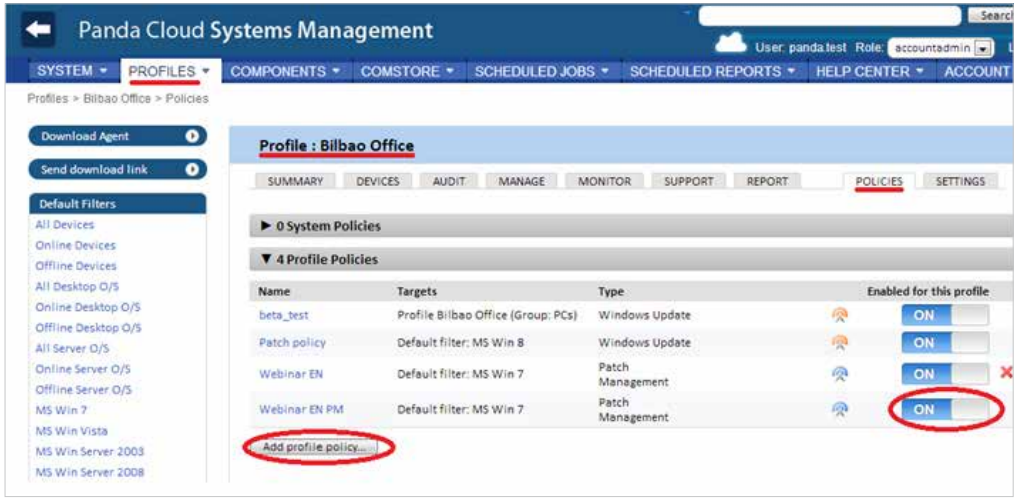


En este caso hemos creado una policy de tipo Agent por lo que en el apartado "Agent Policy Options" se nos pide la información de configuración que afecta a cómo el Servidor PCSM y el usuario van a interactuar con el Agente PCSM instalado en los dispositivos de la red.

En todos los tipos de policy tendremos que configurar el Target, que será un grupo o un filtro ya definido. Como esta es una policy creada en el System Level solo se nos mostrarán los System Device Groups, System Filters y System Profile Groups previamente creados.

¿CÓMO DEFINO UNA PROFILE POLICY?

Desde el Menú General, Profiles, entrando en un Profile concreto y clicando en la Barra de Pestañas, Policies.



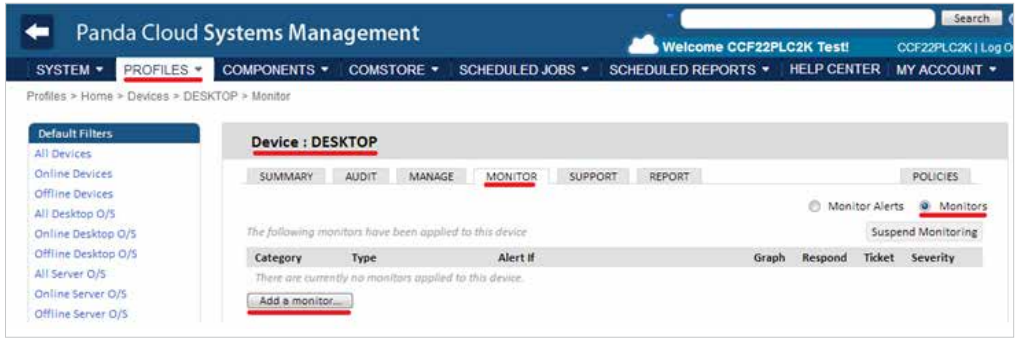
El resto de pasos es idéntico a la creación de una System Policy.

Como ésta es una policy creada en el Profile Level sólo se nos mostrarán los Profile Device Groups y Profile Filters previamente creados.

Para desactivar una Política en el Profile al que afecta pulsamos el botón On / Off bajo "Enabled for this profile".

¿CÓMO DEFINO UNA DEVICE POLICY?.

Desde el Menú Profiles, entrando en un Profile concreto y después en un Device, en la Barra de Pestañas, Monitor y seleccionando Monitors.

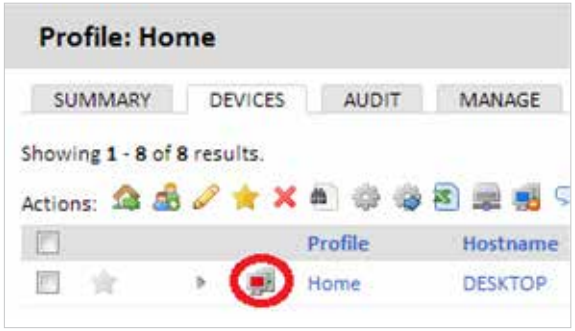


El resto de pasos es idéntico a la creación de una System Policy o Profile Policy.

Al tratarse de una Device Policy no se muestra la posibilidad de elegir Target: la Política únicamente afectara al dispositivo seleccionado.

El botón Suspend Monitoring permite desactivar todos los monitores activos en ese dispositivo; el dispositivo se mostrará en la **Consola PCSM** como Suspendido (suspended).

> Las System Policies y Profile Policies se definen en la Barra de Pestañas, Policies pero las Device Policies se definen en la Barra de Pestañas, Monitor.



TIPOS DE POLICIES

Hay 5 tipos de policy que se resumen a continuación:

- **Agent**
  Este tipo de policy permite determinar la apariencia del **Agente PCSM** así como la funcionalidad expuesta de cara al usuario y al **Servidor PCSM**.

  - **Install Service Only**: oculta el icono en la barra de Tray de forma que el usuario no puede acceder a las ventanas de configuración.
  - **Active Privacy Mode**: la conexión remota al escritorio del dispositivo del usuario requiere una aceptación explicita por parte de éste.
  - **Disable Settings**: el usuario no puede acceder al menú contextual del Agente PCSM.
  - **Disable Audits**: los dispositivos seleccionados no envían datos de auditoría hardware / software.
  - **Disable Incoming Jobs**: impide el envío de jobs al Agente PCSM.
  - **Disable Incoming Support**: deshabilita todo acceso al Agente PCSM por parte del administrador.
  - **Agent Browser Mode**: permite establecer el modo de ejecución del Agente PCSM.

    - **Deshabilitado**.
    - **User**: el **Agente PCSM** no muestra la ventana de Support y por tanto impide el login para entrar en el Modo Administrador.
    - **Administrador**: el **Agente PCSM** se ejecuta de forma completa.

- **Monitoring**
  Esta policy permite añadir procesos de monitorización de los recursos de los dispositivos.

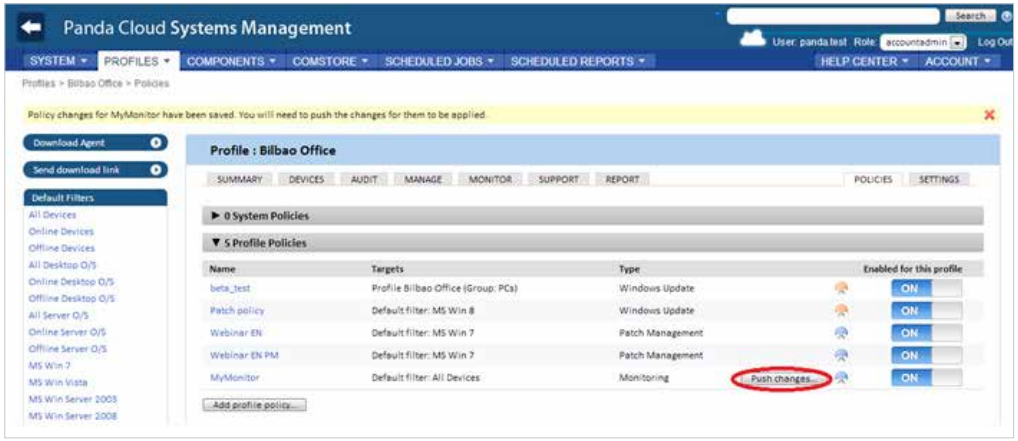
- **Patch Management**
  Patch Management es una de las formas disponibles en **Panda Cloud Systems Management** para descargar y aplicar parches de software.

- **Power**
  Esta policy permite configurar las opciones de ahorro de energía de los dispositivos que las soporten.

- **Windows Update**
  Windows Update es una transposición de las opciones disponibles en un Servidor WSUS y permite configurar las opciones más comunes de Patch Management para sistemas Microsoft.

¿CÓMO DISTRIBUYO UNA POLICY?

Una vez creada la Política se agregará una línea en la pantalla de Policies.



Para distribuir la Política es necesario hacer clic en el botón Push changes. Con esta acción la Política será aplicada distribuida en todos los dispositivos afectados, comenzando su ejecución.

09. MONITORING

¿QUÉ ES?

La monitorización es un tipo de policy dedicado a la detección de fallos en los dispositivos de los usuarios de forma desatendida. De esta manera, el administrador de IT podrá configurar monitores en los dispositivos de usuario que le adviertan de situaciones anómalas y lancen de forma automática alertas o secuencias de script para remediarlas, todo ello sin intervención humana.

COMPOSICIÓN DE UN MONITOR

Un monitor se compone de tres grupos de configuraciones:

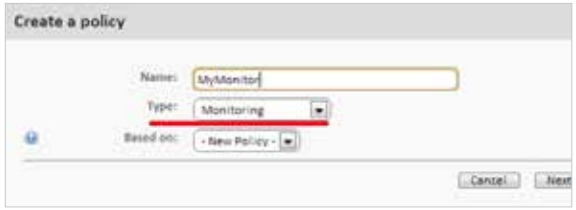
- **Tipo del monitor**: indica su funcionalidad.
- **Condiciones**: parámetros del monitor que describen en qué condiciones desencadenará una respuesta.
- **Respuesta**: acciones automáticas que el monitor puede desencadenar. Son posibles tres tipos de respuesta:

    - Ejecución de componentes.
    - Envío de emails.
    - Generación de Tickets (capitulo 12).

CREACIÓN DE MONITORES

Desde el Menú General, System o desde un Profile concreto en la Barra de Pestañas, Policies hacemos click en Add System/Profile Policy.

En el tipo de policy elegimos Monitoring.



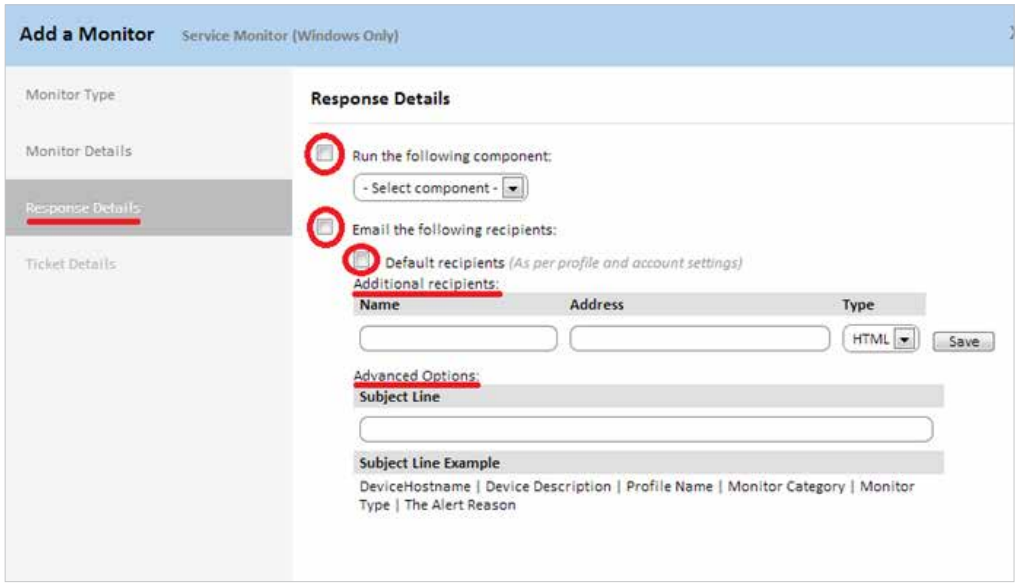
Añadimos un target y un monitor.

> Una policy puede tener más de un monitor asociado.

Al añadir un monitor se mostrará un wizard de cuatro pasos donde se especifica la configuración necesaria.

Paso 1: Monitor Type.

En este paso se indica el tipo de monitor que se añadirá a la policy según sean los recursos objeto de monitorización en el dispositivo del usuario.



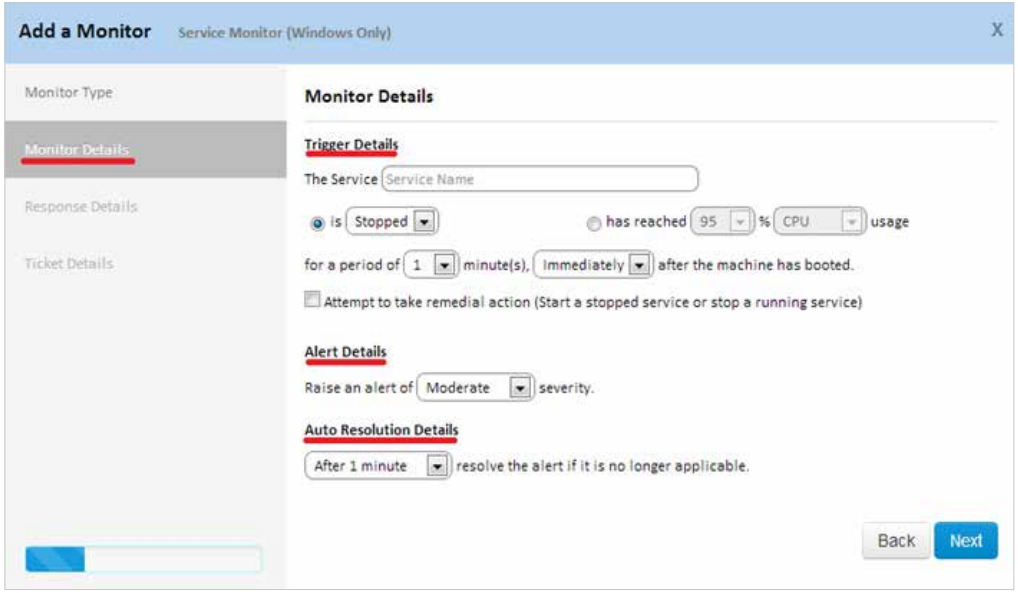
Monitor	Función	Disponible en
Online Status Monitor	Comprueba si el dispositivo está online.	Windows, Mac
CPU Monitor	Controla el consumo de CPU.	Windows, Mac
Memory Monitor	Controla el consumo de memoria.	Windows, Mac
Component Monitor	Lanza un componente de monitorización de la ComStore o diseñado por el administrador	Windows, Mac
Process Monitor	Controla el estado de un proceso concreto	Windows, Mac

Continua

Monitor	Función	Disponible en
Service Monitor	Controla el estado de un servicio concreto.	Windows
Event Log Monitor	Supervisa el visor de sucesos.	Windows
Software Monitor	Supervisa el software que se instala o desinstala del dispositivo.	Windows
Security Center Monitor	Controla el estado del Centro de Seguridad del sistema operativo.	Windows
Disk Usage Monitor	Controla el consumo de disco duro.	Windows
File/Folder Size MonitorMonitor	Controla el tamaño de ficheros y carpetas.	Windows

Paso 2: Monitor Details.

Según su función, cada tipo de monitor necesita de una configuración ligeramente diferente de modo que este paso varía según el tipo de monitor elegido anteriormente.

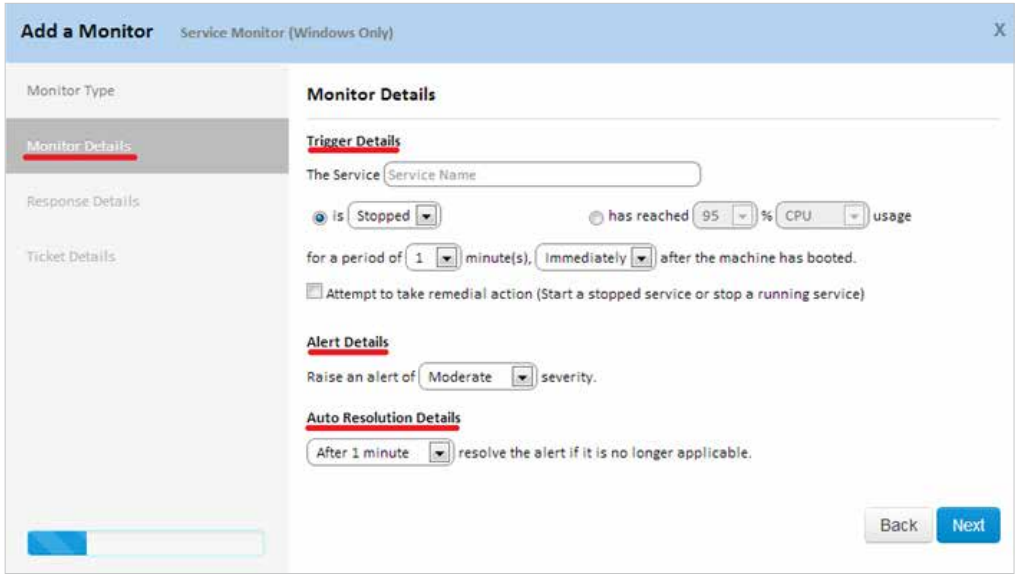


De forma general en este paso se requieren los siguientes datos:

- ✔ **Trigger Details**: configuración complementaria del monitor y condiciones que se tienen que cumplir para que desencadene una respuesta.
- ✔ **Alert Details**: permite elegir la prioridad de la alerta que se generará (Critical, High, Moderate, Low, Information).
- ✔ **Auto Resolution Details**: indica el tiempo que tiene que transcurrir para que una alerta se considere como resuelta de forma automática.

Paso 3: Response Details.

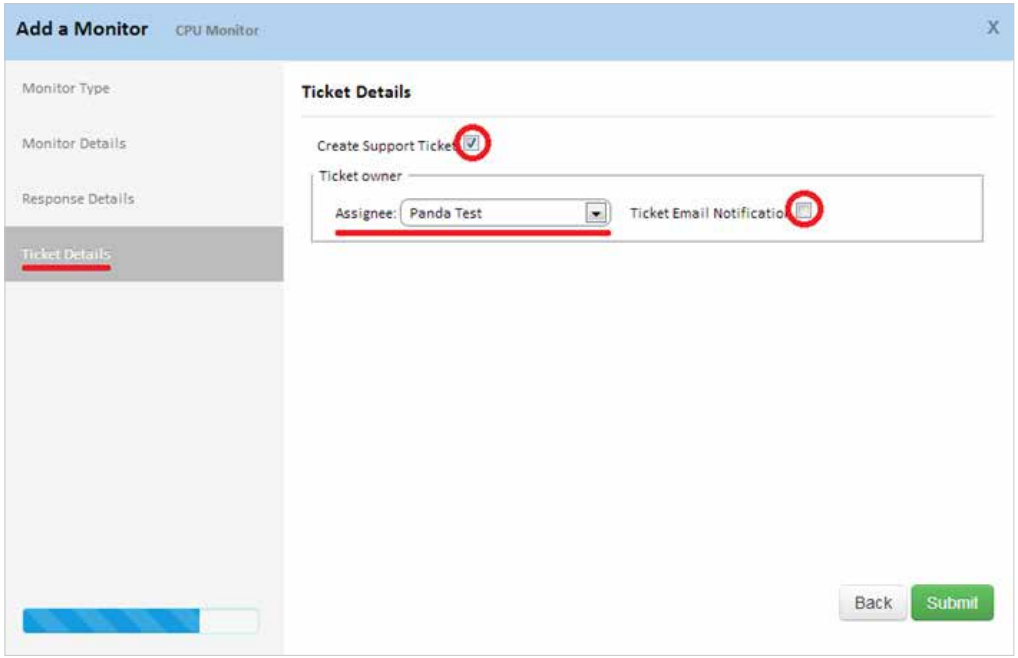
En este paso se indica la respuesta que se desencadenará cuando se alcanzan los límites definidos en el paso 2.



- ✔ **Run the following component:** se mostrarán en el desplegable los componentes importados desde ComStore o desarrollados por el administrador.
- ✔ **Email the following recipients:** permite especificar los destinatarios de los correos, el asunto, el formato y el contenido del mensaje. El check Default recipients permite enviar los correos a las cuentas definidas en la Barra de pestañas, Settings del Profile al que pertenece el monitor creado y a las definidas a nivel global en el Menú general, Account, Setting.

Paso 4: Ticket Details.

En este paso se puede activar la creación automática de tickets como respuesta generada por el monitor al alcanzar los límites definidos en el paso 2.



- **Assignee:** asigna los tickets que el monitor genere a un técnico.
- **Ticket Email Notification:** genera un mail a la cuenta de correo del técnico con los datos generados por el monitor.

10. DESARROLLO DE COMPONENTES

¿POR QUÉ DESARROLLAR COMPONENTES?

El desarrollo de componentes permite al administrador crear nuevos procesos que se ejecutan en los dispositivos de los usuarios y que añaden funcionalidad extra a la **Plataforma PCSM**.

Aunque Por defecto P**anda Cloud Systems Management** ofrece un repositorio de componentes (ComStore) que extiende sus funcionalidades básicas, es posible que sea necesario desarrollar componentes específicos para realizar tareas muy concretas en los dispositivos del usuario.

De este modo **Panda Cloud Systems Management** se presenta como una plataforma de gestión y monitorización remota extensible, que se adapta muy fácilmente a las necesidades particulares de cada cliente.

¿QUÉ REQUISITOS SON NECESARIOS PARA EL DESARROLLO DE COMPONENTES?

En primer lugar se necesitan conocimientos básicos de programación en uno de los lenguajes de scripting soportados:

¿QUÉ REQUISITOS SON NECESARIOS PARA EL DESARROLLO DE COMPONENTES?

En primer lugar se necesitan conocimientos básicos de programación en uno de los lenguajes de scripting soportados:

Lenguaje	Incluido de serie en	Proveedor
Batch	Todas las versiones de Windows.	Microsoft
Visual Basic Script Monitor	Windows 98 y superiores Windows NT 4.0 Option Pack y superiores.	Microsoft
JavaScript (Jscript)	Windows 98 y superiores Windows NT 4.0 Option Pack y superiores.	Microsoft
Powershell	Windows 7.	Microsoft
Python	Mac OS X 10.3 (Panther).	Python Software Foundation
Ruby	Ninguno.	Yukihiro Matsumoto
Groovy	Ninguno.	Pivotal & Groovy Community

Además es necesario que el intérprete asociado al lenguaje de scripting elegido se encuentre instalado y funcionando en el dispositivo del usuario.

Algunos intérpretes como Python o Groovy requieren de su instalación por lo que el funcionamiento de componentes escritos en estos lenguajes no está garantizado en equipos Windows recién instalados.

Como paso previo a la ejecución de un componente desarrollado en un lenguaje no soportado directamente por el dispositivo del usuario, se recomienda ejecutar una tarea de distribución automática del intérprete. La distribución de software será tratada en el capítulo 11.

ARQUITECTURA GENERAL DE COMPONENTES EN PCSM

Los componentes desarrollados para la **Panda Cloud Systems Management** se dividen en tres tipos según su objetivo, comportamiento y forma de ejecución:

- **Applications:**
  Estos componentes facilitan el despliegue de software en la red del cliente. Serán tratados en el capítulo 11.
  Se trata de scripts que se ejecutan por lo general una única vez y llevan asociado al menos un fichero externo, que sería el software a instalar.

- **Monitors**:
  Las Profile Policies o System Policies de tipo Monitor llevan asociado un componente que es el que realiza la monitorización propiamente dicha. De forma general hay tres tipos de componentes de tipo Monitor:

  - **Internos**: accesibles directamente desde la Consola PCSM al crear una policy.
  - **Externos**: son componentes publicados en la ComStore por Panda Security.
  - **Custom**: son componentes desarrollados por el administrador de IT.

Los componentes Externos y Custom se ejecutan en el dispositivo cada 60 segundos.

No es posible cambiar el intervalo de ejecución de un componente Externo o Custom. Si se quiere espaciar la ejecución de un componente Externo o Custom deberá de controlarse dentro del propio componente, por ejemplo almacenando timestamps con la última fecha de ejecución y verificando este valor cada vez que se inicie la ejecución del componente.

- **Applications:**
  Estos componentes facilitan el despliegue de software en la red del cliente. Serán tratados en el capítulo 11. Se trata de scripts que se ejecutan por lo general una única vez y llevan asociado al menos un fichero externo, que sería el software a instalar.

- **Monitors**:
  Las Profile Policies o System Policies de tipo Monitor llevan asociado un componente que es el que realiza la monitorización propiamente dicha. De forma general hay tres tipos de componentes de tipo Monitor:

  - **Internos**: accesibles directamente desde la Consola PCSM al crear una policy.
  - **Externos**: son componentes publicados en la ComStore por Panda Security.
  - **Custom**: son componentes desarrollados por el administrador de IT.

Los componentes Externos y Custom se ejecutan en el dispositivo cada 60 segundos.

No es posible cambiar el intervalo de ejecución de un componente Externo o Custom. Si se quiere espaciar la ejecución de un componente Externo o Custom deberá de controlarse dentro del propio componente, por ejemplo almacenando timestamps con la última fecha de ejecución y verificando este valor cada vez que se inicie la ejecución del componente.

- **Scripts:**
  Son pequeños programas desarrollados en lenguaje de script que se ejecutan en el dispositivo del Cliente. Se pueden ejecutar de forma puntual a través de un job o periódicamente según la programación indicada en el Scheduler.

  En todos los casos una vez cargados los componentes en la plataforma el Servidor PCSM los copiará y ejecutará en todos los dispositivos que sean requeridos.

Tabla resumen

Tipo Componente	Se ejecuta desde	Se ejecuta cada	Objetivo
Applications	Quick Job or Scheduled job.	En el momento o cuando se indique en el calendario.	Despliegue e instalación de software centralizada. La distribución de software será tratada en el capítulo 11.
Monitors	Profile Policy o System Policy.	60 segundos (fijo).	Monitorización de dispositivos.
Scripts	Quick Job or Scheduled Job. **Windows NT 4.0 Option Pack y superiores.**	En el momento o cuando se indique en el calendario.	Ejecución de aplicaciones desarrolladas por el administrador.

Monitors, Applications y Scripts son prácticamente idénticos en lo que a estructura interna se refiere. El tipo de componente únicamente determina cómo se conecta a la **Consola PCSM**. De esta manera, en la creación de un job solo se listarán componentes de tipo Script o Application, y en la creación de un monitor solo aparecerán los componentes de tipo Monitor creados o importados de la ComStore.

CREACIÓN DE UN COMPONENTE DE TIPO MONITOR

Presentación y objetivo del componente

A continuación se detallan los pasos para crear un monitor y distribuirlo en los dispositivos de un Profile concreto.

El objetivo del componente es monitorizar de forma fácil y sencilla la cuarentena del producto de seguridad **Panda Cloud Office Protection**. La cuarentena almacena los ficheros sospechosos de ser malware y también los ficheros detectados como virus, por esta razón resulta de interés para el administrador saber cuántos elementos hay en cuarentena en todo momento.

El ejemplo muestra además lo simple que resulta adaptar e integrar nuevos monitores para otras soluciones software.

A continuación se muestra un resumen de las características del componente.

Dispositivos afectados	Todos los dispositivos Windows 7 del Profile Home.
Lenguaje del script	Visual Basic Script.
Periodicidad del envío de información	Cada 10 minutos se notifica si los elementos de la cuarentena se incrementaron.
Acciones de PCSM	Envío de correo con el resultado de la monitorización al administrador. Generación de alerta automática.

Uno de los problemas con los que habrá que lidiar es que el Agente PCSM ejecutará el script cada 60 segundos de forma automática pero éste solo reportará información cada 10 minutos.

Elementos necesarios

Para seguir este ejemplo es necesaria una licencia de **Panda Cloud Office Protection** y el **Agente PCSM** instalado en un dispositivo aunque, dado que los elementos introducidos en cuarentena por **Panda Cloud Office Protection** son ficheros en una carpeta concreta del dispositivo, en este ejemplo puede usarse con cualquier otra carpeta del sistema.

Panda Cloud Office Protection es una solución Cloud de seguridad, integral y fácil de utilizar que aprovecha todo el potencial de la Inteligencia Colectiva para proporcionar máxima protección en tiempo real contra el spam y las amenazas conocidas a PCs, servidores, portátiles y servidores Exchange.

El componente está desarrollado en Visual Basic Script y por tanto necesitará el intérprete Wscript.exe o Cscript.exe instalado previamente en el dispositivo del usuario. Este intérprete está incluido de serie en todos los sistemas Windows.

Protocolo de comunicación entre el componente y el Servidor PCSM

Prácticamente todos los componentes van a necesitar información del **Servidor PCSM** y enviar de vuelta el resultado de su ejecución. Todos los intercambios de información entre el **Servidor PCSM** y el componente se realizan a través de variables de entorno creadas en el dispositivo.

La creación de estas variables de entorno es ejecutada por el propio **Agente PCSM** de forma automática al lanzar un componente aunque también es usual que sea el propio script el que cree variables de entorno de forma manual para el envío de respuestas al **Servidor PCSM**, que recogerá e incorporará a la **Consola PCSM**.

En este caso se requerirán tres variables de entorno.

Nombre Variable	Dirección	Objetivo
Applications	Lectura.	El script recupera del **Servidor PCSM** el path donde Panda Cloud Office Protection almacena la cuarentena en el dispositivo de cada usuario.
Monitors	Escritura.	Envío de datos al **Servidor PCSM** cada 10 minutos por la salida Estándar.
Scripts	Escritura.	Código de error del script. Si es 0 el **Servidor PCSM** interpreta la monitorización como correcta y no recoge datos de la Salida estándar. Si es 1 **PCSM** interpreta la monitorización como errónea, recoge los datos de la salida estándar (variable Result) y los procesa.

La configuración necesaria para ejecutar el componente en el dispositivo del clienteserá el path de la carpeta a monitorizar. Este path podría ir "hardcoded" en el código fuente del script pero en este ejemplo se tomarán los valores que el administrador haya indicado en la **Consola PCSM**; de esta manera se añade un mayor grado de flexibilidad al componente.

El Errorlevel le indicará al **Servidor PCSM** si tiene que procesar la respuesta del script (variable Result) o no: si el número de ficheros en cuarentena no ha variado o es menor (vaciado de cuarentena) se enviará un Errorlevel 0. Por el contrario si el número de ficheros se ha incrementado entonces se enviará un 1 y se escribirá en la salida estándar (variable Result) cierta información. Para que el **Servidor PCSM** interprete correctamente la salida estándar y pueda extraer el contenido de la variable Result del componente hay que adaptarse al siguiente formato:

```
Linea 1: <-Start Result->
Linea 2: Result=(datos a enviar)
Linea 3: <-End Result->
```

> Si el lenguaje de script elegido es Batch, es necesario añadir el símbolo ^ delante de cada carácter "<" o ">". Por ejemplo
> `^<-Start Result-^>`

Result será la variable de donde el Servidor PCSM extraerá los datos al terminar la ejecución del componente. El string que quede a la derecha del "=" es el contenido que el Servidor PCSM almacenará y procesará.

Esquema de funcionamiento general

- Paso 1: carga del componente de tipo monitor en la **Plataforma PCSM**.
- Paso 2: distribución del monitor mediante System Policies o Profile Policies.
- Paso 3: ejecución del componente cada 60 segundos.
- Paso 4: envío de información cada 10 minutos y procesamiento en la **Plataforma PCSM**.

Paso 1: carga del componente de tipo monitor en la plataforma PCSM

En el Menú General, Components, Add Component.

Seleccionar el tipo de script Monitors.

Seleccionar el lenguaje de scripting a utilizar, en este ejemplo VBScript.

Establecemos el tiempo máximo de ejecución del componente. Pasado ese tiempo el **Agente PCSM** interrumpirá su ejecución.

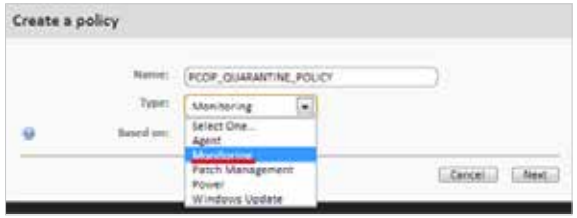
> Se recomienda desarrollar componentes muy ligeros, que tarden muy poco tiempo en ejecutarse.

Establecemos las variables de entrada y salida, en este ejemplo PCOP_PATH contendrá el path donde se encuentra la carpeta de cuarentena de **Panda Cloud Office Protection**. Result contendrá la salida del script.

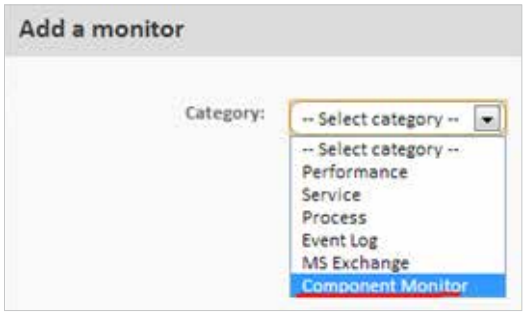
Haciendo click en Save el componente quedará agregado al repositorio de la cuenta.

Paso 2: distribución del monitor mediante System Policies o Profile Policies

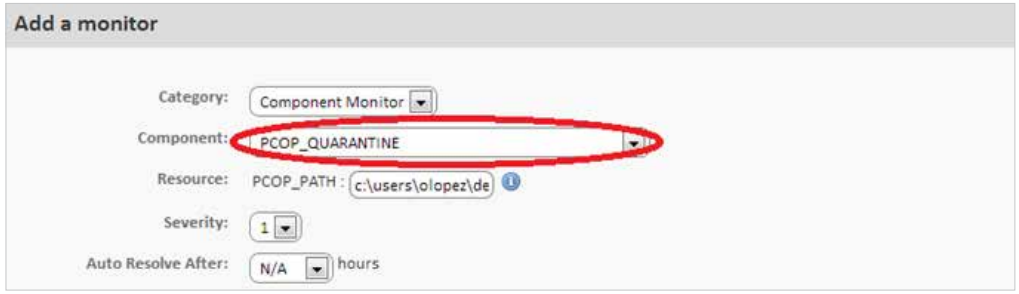
En el caso del desarrollo de un monitor, es necesaria la creación de una Profile Policy o System Policy de tipo Monitoring.



Añadir el target Windows 7 y un monitor de tipo Component Monitor.

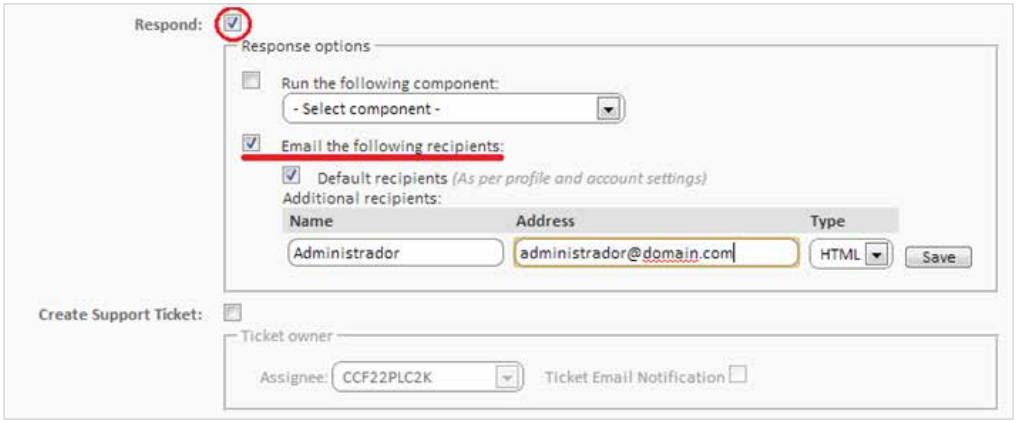


Seleccionar el componente recién creado y salvar.

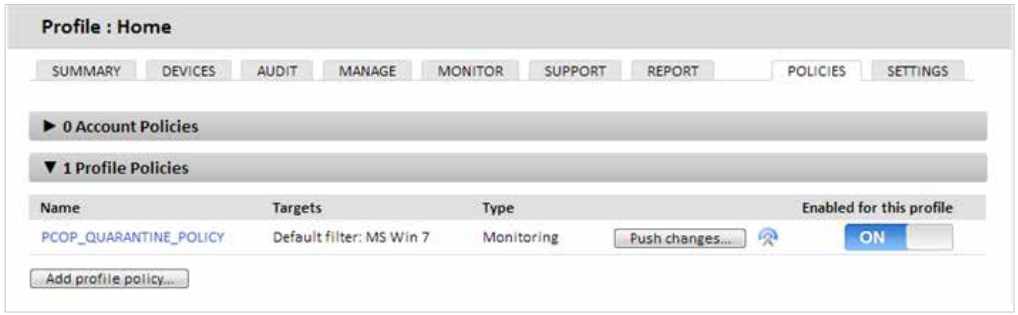


Se puede indicar la Severidad de la alerta que **PCSM** creará cuando el monitor devuelva una condición de error y si esta alerta se auto resuelve por sí misma al cabo de un tiempo, o por el contrario se resuelve de forma manual por el administrador (N/A).

Para que el **Servidor PCSM** genere un correo cuando se detecten nuevos elementos en la cuarentena definir una Respuesta (Respond) de tipo Email con la dirección de correo del destinatario. El contenido de la variable de respuesta Result será copiada en el correo que se envía al administrador.



Una vez creado el monitor se añadirá una línea en la pantalla de Policies.



Para distribuir el monitor es necesario hacer clic en el botón Push changes. Con esta acción la política será aplicada y el monitor será distribuido en todos los dispositivos afectados, comenzando su ejecución.

Paso 3: creación de variables de entorno y ejecución del componente cada 60 segundos

Una vez de distribuido el monitor en los dispositivos éste se ejecutará cada 60 segundos. Para ello se invoca el intérprete de script asociado, se leen las variables de entorno necesarias y se escribe la respuesta adecuada.

> El código fuente completo del script se encuentra en el Apéndice A.

En la línea 24 lee la variable de entorno PCOP_PATH y obtiene un objeto de tipo FileSystemObject que apunta a la carpeta de la cuarentena.

```
23      Set WshSysEnv = WshShell.Environment("PROCESS")
24      Set objFolder = objFSO.GetFolder(WshSysEnv("PCOP_PATH"))
```

Las líneas 25 a 30 controlan si la variable de entorno está definida. Si la variable no fue definida en la **Consola PCSM** se revuele un error en la variable Result y se termina la ejecución con Errorlevel 1 (línea 34).

```
25    if err.number <> 0 then
26        'PCSM didn't send the environment variable
27        err.clear
28        WScript.Echo "<-Start Result->"
29        WScript.Echo "Result=PCOP_PATH variable not defined on PCSM console or path not four
30        WScript.Echo "<-End Result->"
31        Set WshShell = nothing
32        Set WshSysEnv = nothing
33        Set objFolder = nothing
34        WScript.Quit(1)
```

En las líneas 44-51 se escribe en el Registry del dispositivo el número de elementos de la carpeta monitorizada. Puesto que el script se ejecuta cada 60 segundos pero se quiere realizar la comparación cada 10 minutos se almacenan 10 entradas en el registro con el valor registrado cada 60 segundos.

```
44      While Err.Number=0 And n < 10
45          iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor" & n))
46          If err.number<>0 then
47              WshShell.RegWrite "HKLM\Software\Panda Security\Monitor" & n, colFiles.count, "REG_SZ"
48          Else
49              n=n+1
50          End If
51      Wend
```

La ejecución de componentes en el dispositivo del usuario es "atómica": no se conserva el estado entre dos ejecuciones sucesivas del mismo script. Si se requiere de varias ejecuciones de un mismo script para generar un resultado válido los estados intermedios deberán de ser guardados en los dispositivos y leídos en cada ejecución del componente.

Se recomienda utilizar el registro para almacenar el estado entre dos o más ejecuciones del componente dentro de un dispositivo aunque también pueden utilizarse ficheros temporales.

Cuando el contador es igual a 9 (10 anotaciones en el Registro, 10 minutos) se compara el valor inicial con el final (línea 57). Si es mayor en las líneas 59, 60 y 61 se envía la diferencia y se termina el script con Errorlevel 1.

Terminado el último ciclo se borran todas las entradas del Registro (Líneas 64-66) y se copia la última entrada como la primera para continuar con el proceso.

```
54      If n=9 Then
55          iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor0"))
56          iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda Security\Monitor9"))
57          if iCountPast < iCountNow then
58              'there is more items in the folder, it updates the registriy and sends an alert
59              WScript.Echo "<-Start Result->"
60              WScript.Echo "Result=" & iCountNow - iCountPast & " new items in PCOP quarantine"
61              WScript.Echo "<-End Result->"
62              bHit=true
63          end if
64          For n=0 To 9
65              WshShell.RegDelete("HKLM\Software\Panda Security\Monitor" & n)
66          Next
67          WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0", colFiles.count, "REG_SZ"
68
69      end if
```

Paso 4: envío cada 10 minutos de la salida estándar y procesamiento en la plataforma PCSM

Si el script termina la ejecución con Errorlevel 0 la respuesta no es tenida en cuenta por el Servidor PCSM, si termina con Errorlevel 1 el Servidor PCSM leerá la salida estándar en busca de la variable Result entre las cadenas "<-Start Result->" y "<-End Result->". Con esta información realizará las acciones configuradas en la definición del monitor.

Cómo utilizar variables globales

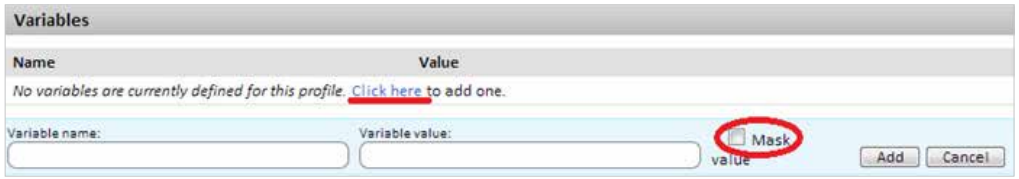
Si el desarrollo de nuevos scripts es frecuente, es muy probable encontrarnos en la situación de querer utilizar datos comunes en todos ellos, como pueden ser paths a carpetas concretas en los discos duros del usuario, letras de unidades de red compartidas en servidores o incluso credenciales comunes para ejecutar ciertas tareas.

Una posible solución es incorporar en cada script todos los datos que se necesiten de tal forma que si la información cambia habría que actualizar manualmente todos los scripts desarrollados y volverlos a distribuir entre los dispositivos.

La opción más conveniente sin embargo es definir variables globales a nivel Profile o System para que puedan ser utilizados por los scripts de forma directa.

De esta manera en el Menú General, System, Settings o Menú Profile, Settings podemos definir variables y su contenido, que será directamente accesible desde los scripts que diseñemos cuando se ejecuten en los dispositivos de los usuarios.

En el caso de almacenar información sensible como usuarios y contraseñas podemos marcar la casilla "mask" para sustituir el contenido de la variable por asteriscos en la **Consola PCSM**.



Al hacer la distribución de los scripts el **Servidor PCSM** enviará el contenido de las variables al **Agente PCSM**, que se encargará de crear variables de entorno en el dispositivo de usuario fácilmente accesibles por los scripts que hayamos diseñado.

Cómo mostrar el estado de un dispositivo en la Consola PCSM

En el paso 2 del ejemplo se indicaba qué tareas tienen que desencadenarse en el **Servidor PCSM** cuando el resultado de componente es "error"; en este caso se mandaba un correo al administrador informando del cambio de estado del dispositivo.

Este enfoque es correcto en el caso de un dispositivo que cumple una condición de error o excepción y el administrador quiere ser informado de ello sin necesidad de tener que consultar la **Consola PCSM** cada cierto tiempo. Sin embargo puede ser necesario simplemente visualizar el estado de un dispositivo sin atender a condiciones de error, para ello será necesario publicar los datos de interés en la **Consola PCSM**.

Para este escenario el componente utilizará los campos Custom Fields de la **Consola PCSM** que aparecen en la Barra de Pestañas, Summary del Device Level de cada dispositivo.

La etiqueta "Custom Field 1" y sucesivas (hasta 5) se pueden renombrar a nivel global para todos los dispositivos que administre el partner independientemente del Profile al que pertenezcan, o se puede definir al nivel de Profile concreto:

- ✔ En el System Level en el Menú General, Account, Settings.
- ✔ En el Profile Level en la Barra de Pestañas, Settings.

Custom Field	System Label	Account Override
1	Custom field 1	try
2	Custom field 2	Custom field 2
3	Custom field 3	Custom field 3
4	Custom field 4	Custom field 4
5	Custom field 5	Custom field 5

El contenido de los Custom Fields se toma de las ramas del registro de cada dispositivo, indicadas a continuación:

- HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom1
- HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom2
- HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom3
- HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom4
- HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage\Custom5

Cada una de las ramas indicadas podrá contener un string de hasta 255 caracteres.

Un componente podrá escribir libremente en las ramas del registro indicadas de forma que el **Agente PCSM** las leerá al lanzar una auditoria automática (cada 24 horas) o manual (bajo demanda) y enviará la información al **Servidor PCSM**, que se encargará de mostrarla en la **Consola PCSM**. Además el **Agente PCSM** procederá al borrado de esta información en el Registro del dispositivo una vez leída y enviada al **Servidor PCSM**.

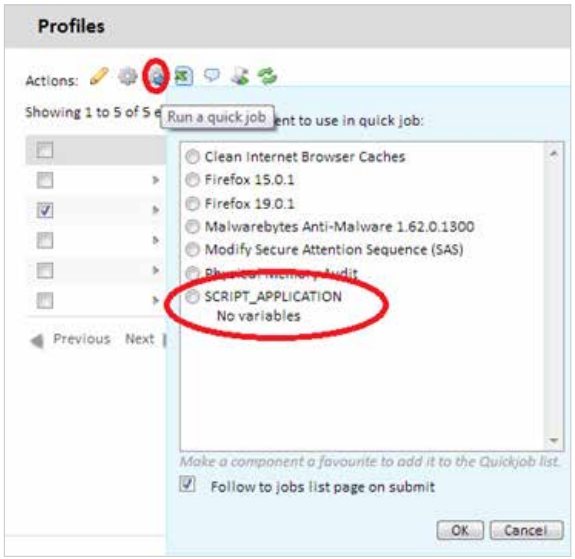
CREACIÓN DE UN COMPONENTE DE TIPO SCRIPT

La creación de un componente de tipo Script es exactamente igual a la de un monitor. Se elige en primer lugar el tipo Script al crear el componente.

La pantalla de configuración solo difiere de la de Monitors en la zona de recogida de información: no podremos definir variables de salida pero en su lugar se permite buscar cadenas en la Salida estándar (stdout) o Salida de error (stderr) para activar condiciones de Warning en la **Consola PCSM**.

Con esto aparecerá en los listados de Quick Jobs y jobs.

Haciendo click en Ok el componente se ejecutará de forma inmediata.



11. DISTRIBUCIÓN E INSTALACIÓN CENTRALIZADA DE SOFTWARE

OBJETIVO DE LA INSTALACIÓN CENTRALIZADA DE SOFTWARE

El **Servidor PCSM** puede distribuir ficheros y paquetes de software de forma automática entre todos los dispositivos administrados de la red. De esta manera el administrador puede garantizar que todos los dispositivos que administra tienen instalado el software o documentos necesarios para que los usuarios puedan trabajar, sin necesidad de desplazarse o conectar por acceso remoto a cada dispositivo de forma individual. La distribución de software de forma automática ayudará al administrador a mantener el software libre de vulnerabilidades (Java, Adobe, etc.) reduciendo así de forma considerable el riesgo de infección y la pérdida de información confidencial.

REQUISITOS PARA LA INSTALACIÓN CENTRALIZADA DE SOFTWARE

La distribución e instalación de software es un proceso que se ejecuta a través de componentes de tipo Application.

Al igual que los componentes de tipo Monitor y Script explicados en el capítulo 10, los componentes Application constan de un pequeño script, que en este caso no tiene otro objetivo que el de guiar el proceso de instalación, y de una serie de ficheros y/o programas a instalar.

Para cada grupo de ficheros o programas a instalar en los dispositivos de usuario será necesario crear un componente independiente.

PROCEDIMIENTO PARA DISTRIBUIR E INSTALAR PAQUETES

El procedimiento general consta de 4 pasos:

1. Determinar los dispositivos sobre los cuales se instalará el software.

El procedimiento para encontrar los dispositivos que no tienen los ficheros o programas instalados varía dependiendo de si el Servidor PCSM puede realizar una auditoría de programas instalados en el dispositivo o no.

Si el software a instalar aparece en la lista de programas instalados mantenida por el propio sistema operativo también se mostrará en las auditorias de software de PCSM y por tanto será posible crear un filtro que discrimine los dispositivos que ya tengan instalado el software.

Si el software no tiene instalador y por tanto no aparece en la lista de programas instalados o si se trata de documentos sueltos, ficheros de configuración etc el Servidor PCSM no será capaz de filtrar dispositivos que ya tengan estos ficheros instalados y será el propio script de instalación el que tenga que realizar las comprobaciones oportunas de forma manual.

2. Generar un componente de instalación de software.

Los pasos involucrados son los mismos que los descritos en el capítulo 10 para la creación de componentes de tipo Script o Monitor.

3. Lanzar un job para empujar el componente de instalación a los Agentes de los dispositivos afectados.

Se puede lanzar un job programado para cierta fecha en la que el usuario no esté trabajando con el dispositivo, con el objetivo de minimizar el impacto en el rendimiento.

4. Recoger el resultado del despliegue para determinar posibles fallos.

Una vez terminado el proceso es posible recoger un código de error y/o mensaje que muestre en la **Consola PCSM** el resultado del despliegue.

Se distinguen cuatro estados finales:

- ✔ Success: la ejecución del despliegue fue completada sin errores. El script devuelve el código de Errorlevel 0.
- ✔ Success - Warning: la ejecución del despliegue fue completada con algunos errores no importantes. El script devuelve el código de Errorlevel 0 y un string por la Salida Estándar o Error Estándar que será interpretada por la Consola PCSM.
- ✔ Error: la ejecución del despliegue no se completó. El script devuelve el código de Errorlevel 1.
- ✔ Error - Warning: la ejecución del despliegue no se completó. El script devuelve el código de Errorlevel 1 y un string por la Salida Estándar o Error Estándar que será interpretada por la **Consola PCSM**.

EJEMPLOS DE DESPLIEGUE

Para ilustrar la distribución de software se proponen cuatro ejemplos:

1. Distribución de documentos mediante lenguaje de script.
2. Distribución de documentos sin lenguaje de script.
3. Distribución de software autoinstalable.
4. Distribución de software sin instalador.

> Los procedimientos aquí mostrados así como las herramientas de terceros utilizadas y lenguajes de script son ejemplos y pueden cambiar. Panda Cloud Systems Management está pensando para ser flexible y adaptarse a las herramientas con las que el Administrador se encuentre más cómodo.

Distribución de documentos mediante lenguajes de script

El objetivo de este ejemplo es distribuir una carpeta en el directorio raíz del dispositivo del usuario tres documentos de tipo Word. Para ello se siguen los siguientes pasos:

1. Determinar los dispositivos sobre los que se instalará el software.

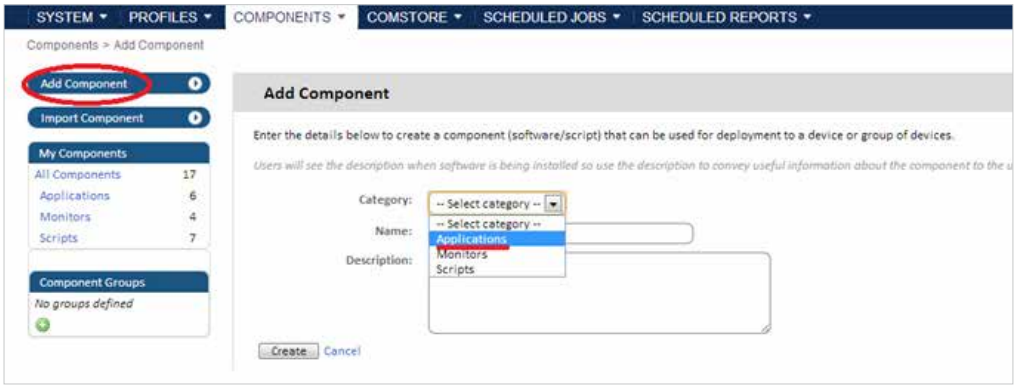
Como en este caso el Servidor PCSM no tiene visibilidad sobre el estado del disco duro del dispositivo del usuario a nivel de sistema de ficheros, el script de instalación se distribuirá entre todos los dispositivos del Profile y será el propio script (líneas 19-24) el que compruebe si la carpeta con los documentos existe o no.

```
19      Set objFolder = objFSO.Getfolder(CONST_PATH)
20      If Err.Number=0 Then
21          'the folder already exists, the files won't be copied
22          WScript.Echo "Deploy unsuccessful: The folder already exists"
23          WScript.Quit (0)
24      End If
```

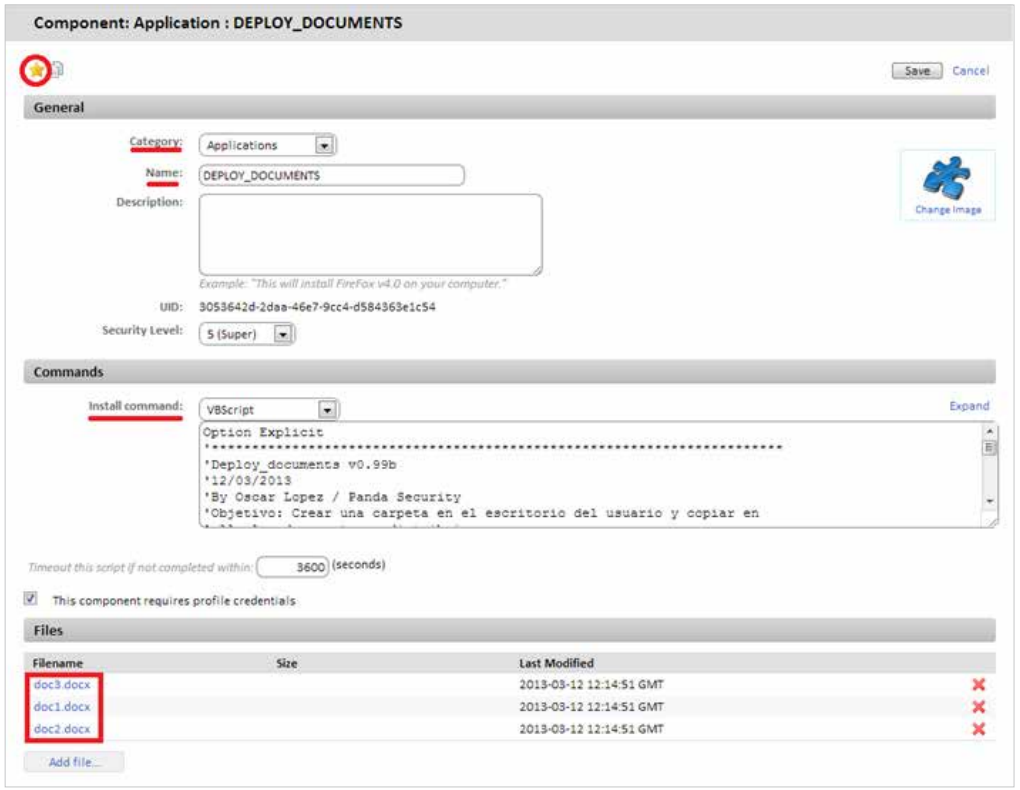
Si la carpeta no existe se crea (línea 28), se mueven los documentas a ella (líneas 30-32) y se enviará un mensaje por la Salida Estándar (línea 37).

```
28      Set objFolder = objFSO.CreateFolder(CONST_PATH)
29      'the documents will be moved to the folder
30      objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31      objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32      objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33      If Err.Number<>0 Then
34          WScript.Echo "Deploy unsuccessful: " & Err.Description
35          WScript.Quit (1)
36      Else
37          WScript.Echo "Deploy successful: All files were copied"
38          WScript.Quit (0)
39      End If
```

2. Generar un componente de instalación de software.



Se agrega un componente de tipo Applications donde añadimos los documentos a distribuir y el script que creará la carpeta y moverá los tres documentos en cada uno de los dispositivos.



En la pantalla de Component: Application es importante indicar:

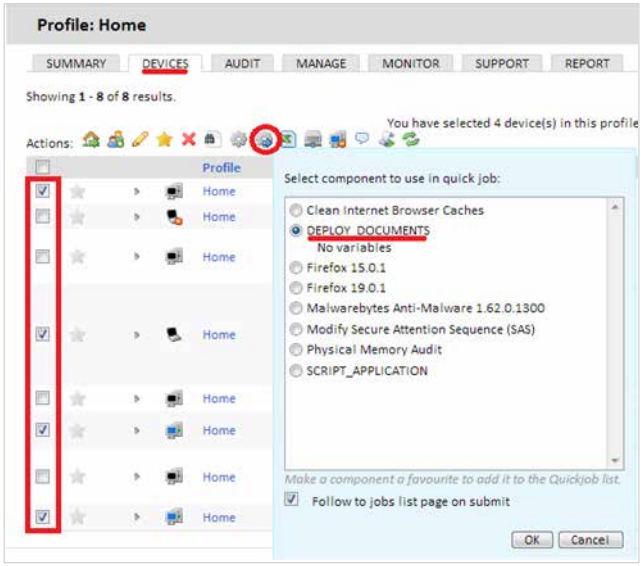
- ✔ El componente es Favorito para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- ✔ La categoría (Applications) del componente y su nombre.
- ✔ El lenguaje de script utilizado (Install command).
- ✔ Agregar los documentos a distribuir en la sección Files.

En la zona de Post-Conditions se pueden indicar cadenas de texto que serán interpretadas por la **Consola PCSM** como Warnings.

En el ejemplo se indica que si en la Salida Estandar (Resource:stdout) se encuentra (Qualifier:is found in) la cadena "Deploy unsucessfull" el resultado de la ejecución del script será considerado como Warning.

3. Lanzar un job para empujar el software a los Agentes de los dispositivos afectados.
Se hace clic en Quick Job o job con los dispositivos del Profile donde se quiere desplegar los documentos seleccionados.

> En el System Level se permite seleccionar Profiles completos sobre los cuales aplicar la distribución de software.



4. Recoger el resultado del despliegue para determinar posibles fallos.
Las condiciones de salida definidas en el script de ejemplo son 3:

- Success: los ficheros con copiados sin errores en la carpeta destino (líneas 30-32). Se termina con un Errorlevel 0 (línea 38).

```
28      Set objFolder = objFSO.CreateFolder(CONST_PATH)
29      'the documents will be moved to the folder
30      objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
31      objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
32      objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
33      If Err.Number<>0 Then
34          WScript.Echo "Deploy unsuccessful: " & Err.Description
35          WScript.Quit (1)
36      Else
37          WScript.Echo "Deploy successful: All files were copied"
38          WScript.Quit (0)
39      End If
```

- Error: se produce algún error en la copia de ficheros. Se termina con un Errorlevel 1 (línea 35).

- Success - Warning: la carpeta ya existe de forma que los ficheros no se copian. Se termina con un Errorlevel 0 (línea 23) y se genera la cadena "Deploy unsuccessful" que el **Servidor PCSM** interpretara como Warning tal y como se configuró en la zona Post-Conditions del paso 3.

```
19      Set objFolder = objFSO.Getfolder(CONST_PATH)
20      If Err.Number=0 Then
21          'the folder already exists, the files won't be copied
22          WScript.Echo "Deploy unsuccessful: The folder already exists"
23          WScript.Quit (0)
24      End If
```

Una vez lanzado el job aparecerá en Menú General, Scheduled Jobs, Active Jobs.

En la Barra de Pestañas, Completed Jobs podremos ver el resultado del despliegue, a Rojo si terminó con Error, Naranja si hubo un Warning o a Verde si fue Successful.

Los iconos Stdout y Stderr muestran una copia de la Salida Estándar y Error Estándar generado por el propio script.

Además en esta pestaña tenemos una Barra de Iconos que nos permitirán desencadenar varias acciones:

- En la zona Actions se agrupan los iconos que permiten relanzar el job, recargar la página para actualizar el estado del job o descargar en un fichero la Salida y Error Estándar.

- Con el filtro Views se pueden filtrar los jobs según su estado.

Distribución de documentos sin lenguaje de scripting

Puede simplificarse el script de instalación enormemente si no son necesarias comprobaciones previas ni generación de advertencias en la **Consola PCSM**.

En este ejemplo distribuiremos los 3 documentos del ejemplo anterior pero esta vez en vez de generar la estructura de carpetas desde el script, simplemente crearemos un paquete .EXE autoextraíble con los documentos comprimidos y la estructura de carpetas en su interior que consideremos oportuna. La generación del paquete .EXE puede hacerse con muchas herramientas, en este ejemplo usamos WinRar.

Para descargar una versión gratuita de WinRar visitar la página http://www.winrar.com

En este ejemplo se va a generar un fichero .EXE auto extraíble con las siguientes características:

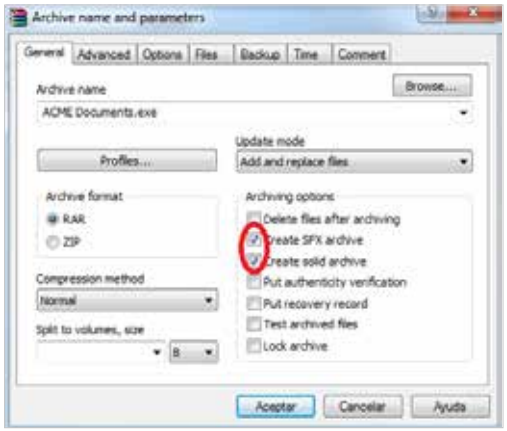
- ✔ Funcionamiento en modo "Silent".
- ✔ La carpeta con el contenido será creada de forma automática en C:\.
- ✔ Si la carpeta existiera previamente se sobrescribirá su contenido sin avisar.

Es imprescindible generar un fichero auto extraíble que funcione en modo "Silent", es decir, que no muestre diálogos ni ventanas ni requiera de la interacción del usuario.

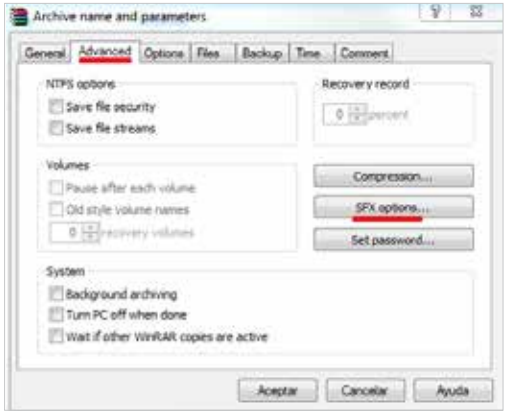
Pasos para generar un fichero autoextraíble de instalación "Silent".

- ✔ **Paso 1**: preparar la carpeta con los documentos a distribuir. Crear la carpeta raíz "ACME Documents" del ejemplo y en su interior colocar todos los ficheros, carpetas y subcarpetas que se necesiten distribuir.

- ✔ **Paso 2**: generar el ejecutable. Con el programa WinRar abierto arrastrar la carpeta recién creada "ACME Documents" y marcar las opciones "Crear un archivo autoextraíble" y "Crear un archivo solido".

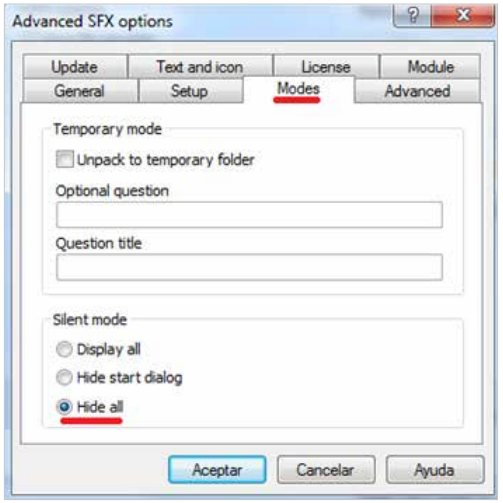


- ✔ **Paso 3**: configurar el ejecutable como "Silent". Para ello activamos Ocultar Todo en Avanzado -> Autoextraíble -> Modos -> Mostrar.

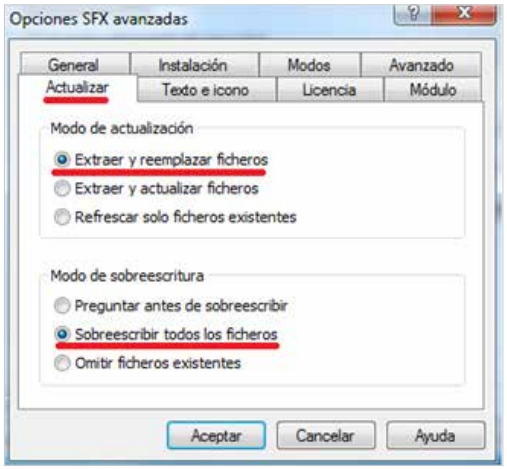


- ✔ **Paso 4**: indicar el path de destino donde se creara la carpeta en la pestaña General.

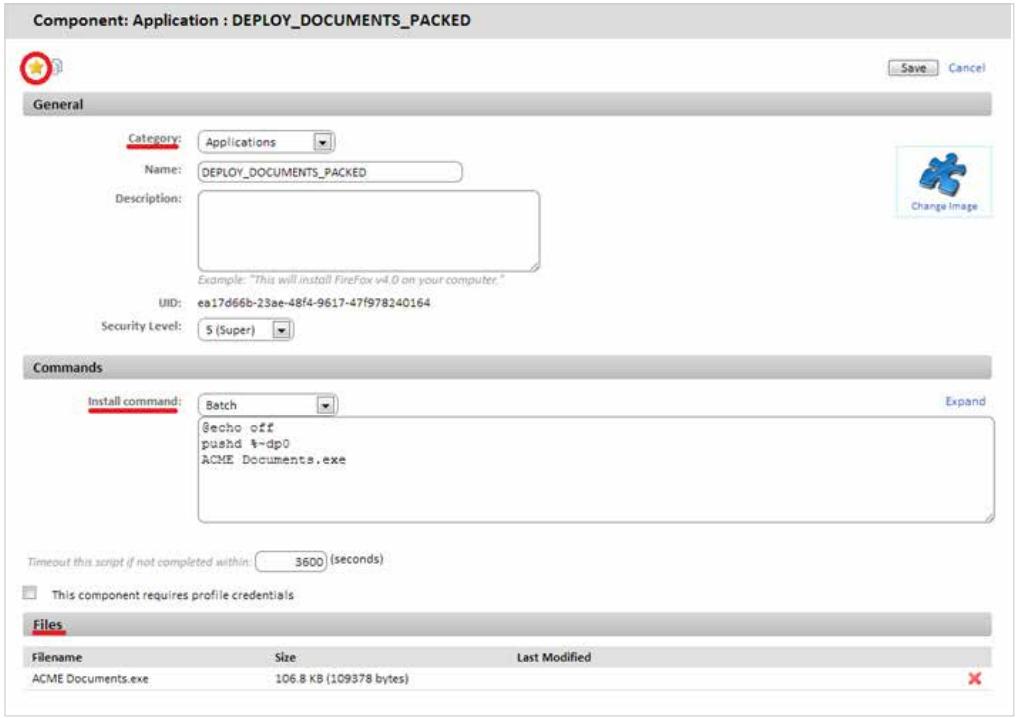
- ✔ **Paso 5**: indicar que se sobrescribirán los ficheros en caso de existir previamente sin preguntar nada al usuario.



- **Paso 5**: indicar que se sobrescribirán los ficheros en caso de existir previamente sin preguntar nada al usuario.



Una vez generado el paquete "ACME Documents.exe" se creará un componente Application para su distribución.



En la pantalla de Component: Application es importante indicar:

- El componente es Favorito para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda) .
- La categoría (Applications) y el nombre del componente.
- El lenguaje de script utilizado (Install command), en este caso Batch.
- Agregar el paquete a instalar "ACME Documents.exe".

Simplemente el script ejecuta el paquete auto extraíble que se encargará de crear la carpeta en la unidad C:\ junto con toda su estructura interna, machacando cualquier contenido anterior.

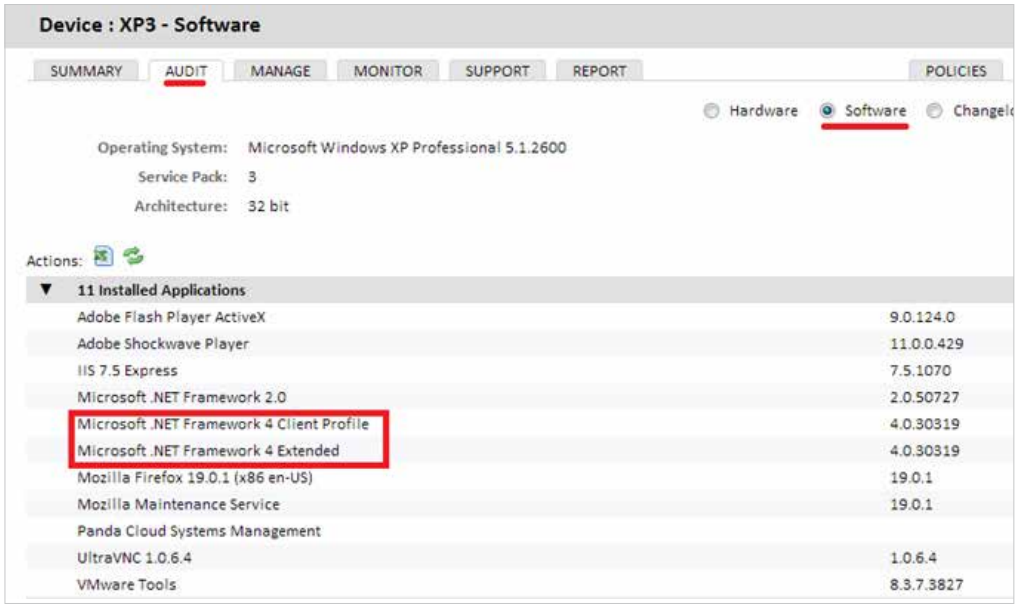
Distribución de software autoinstalable

En este ejemplo se desplegará el paquete Framework .NET 4.0 dotNetFx40_Full_x86_x64.exe de Microsoft en aquellas máquinas que no lo tengan ya instalado.

Para ello, y dado que Microsoft Framework .NET 4.0 es un programa que sí aparece en el listado de programas mantenido por el sistema operativo del dispositivo, utilizaremos un filtro para discriminar aquellos que no lo tengan instalado.

El paquete de instalación es un .EXE auto extraíble que acepta los parámetros /q /norestart para ejecutarse en modo "Silent" y evitar el reinicio del dispositivo de forma que no será necesaria ninguna preparación especial adicional.

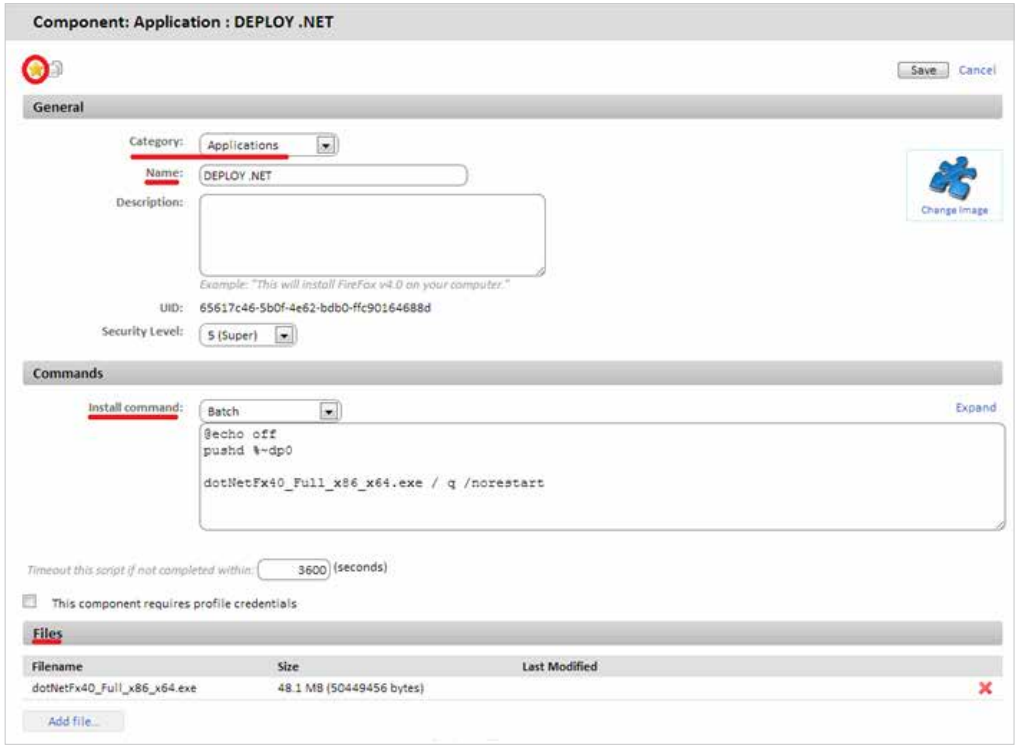
1. Determinar los dispositivos sobre los cuales se instalará el software.
Para filtrar todos los dispositivos que ya tienen instalado el software es necesario conocer qué cadena de identificación se corresponde al paquete ya instalado. Este dato se puede obtener en la Barra de Pestañas, Audit, Software de un dispositivo que ya tenga instalado el paquete.



Con este dato se crea un Profile Filter o un System Filter con la siguiente configuración:

- ✔ **Field:** software package para inspeccionar el software instalado en el dispositivo.
- ✔ **Search Item**: aquí se indica la cadena que identifica el software que queremos instalar.
- ✔ **Condition**: Does not contain para seleccionar aquellos dispositivos que no contengan en el campo Software package el contenido especificado en Search Item.

2. Generar un componente de instalación de software.
La generación del componente de instalación es extremadamente sencilla.



En la pantalla de Component: Application es importante indicar:

- ✔ El componente es Favorito para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda).
- ✔ La categoría (Applications) y el nombre del componente.
- ✔ El lenguaje de script utilizado (Install command), en este caso Batch.
- ✔ Agregar el paquete a instalar "dotNetFx40_Full_x86_x64.exe".

El script únicamente tiene una línea relevante, que es la que ejecuta el paquete de instalación con los parámetros necesarios para conseguir una instalación "Silent".

3. Lanzar un job para empujar el software a los Agentes de los dispositivos afectados.
Primero se seleccionado el filtro previamente preparado y después se ejecutará un job con la application creada.

4. Recoger el resultado para determinar posibles fallos.
Una buena manera de comprobar el resultado de la instalación es revisando el filtro de dispositivos previamente preparado para ver si el número de dispositivos que no tiene instalado el software desplegado es menor. Todos aquellos dispositivos que sigan apareciendo en el filtro habrán tenido algún tipo de error.

> La información de auditoría de dispositivos con el contenido del hardware y software instalado es enviada por el **Agente PCSM** al **Servidor PCSM** cada 24 horas de forma que la lista de software recién instalado no se actualizará hasta pasado ese tiempo. No obstante se puede forzar una actualización manual con la acción Request device audit de la Barra de Acciones.

Distribución de software sin instalador

Muchos programas están formados por un único ejecutable sin instalador asociado que genere la estructura necesaria en el menú Inicio ni los accesos directos en el escritorio ni las entradas pertinentes en Añadir y Quitar programas. Este tipo de programas puede ser distribuido siguiendo el ejemplo de distribución de documentos o de paquete auto extraíble; sin embargo hacerlo de esta manera impide al **Servidor PCSM** generar una auditoria de programas instalados fiable ya que no aparecerán en el listado de programas instalados mantenidos por el sistema operativo del dispositivo.

Por esta razón frecuentemente se recurren a herramientas de terceros que generan un único paquete MSI con todos los programas que queramos añadir, creando los grupos necesarios en el menú Inicio y los accesos directos en el escritorio del usuario para facilitar su ejecución.

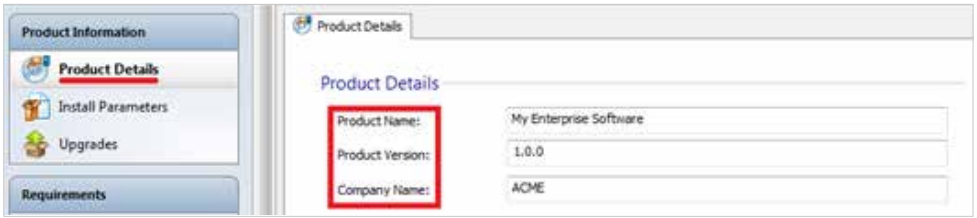
Para realizar esta labor se utilizará en este caso el programa Advanced Installer, que en su versión gratuita nos permite generar instaladores MSI de forma simple.

> Para descargar la versión gratuita de Advanced Installer visitar la página http://www.advancedinstaller.com/download.html

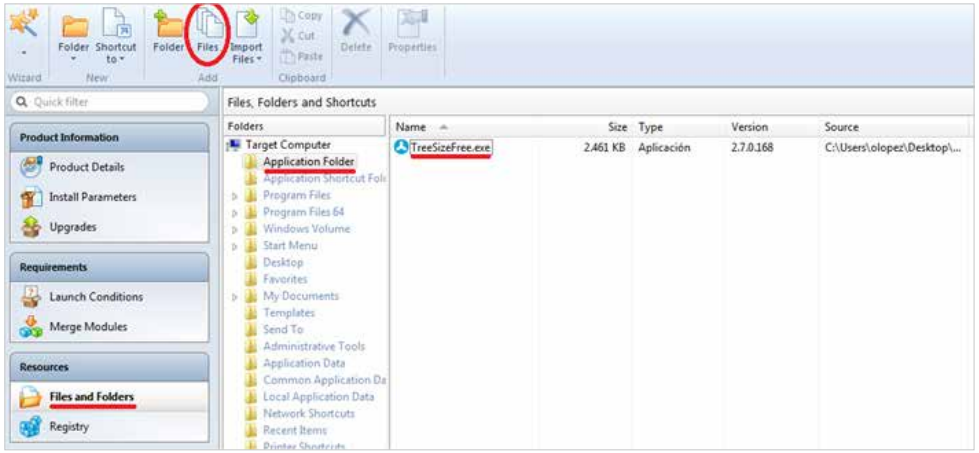
Para generar el instalador se siguen los siguientes pasos:

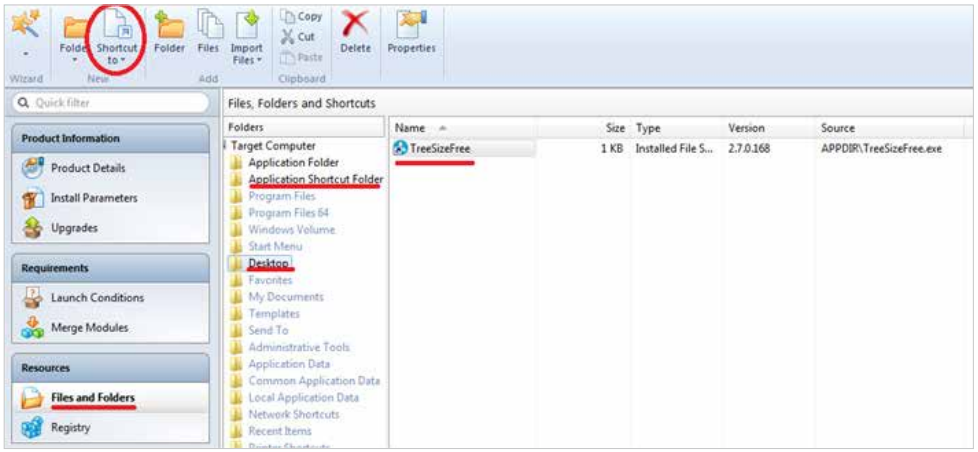
- ✔ Elegir el template Simple (gratuito).

- ✔ En Products Details se rellenan los datos básicos del instalador: Product Name, Product Version y Company Name.



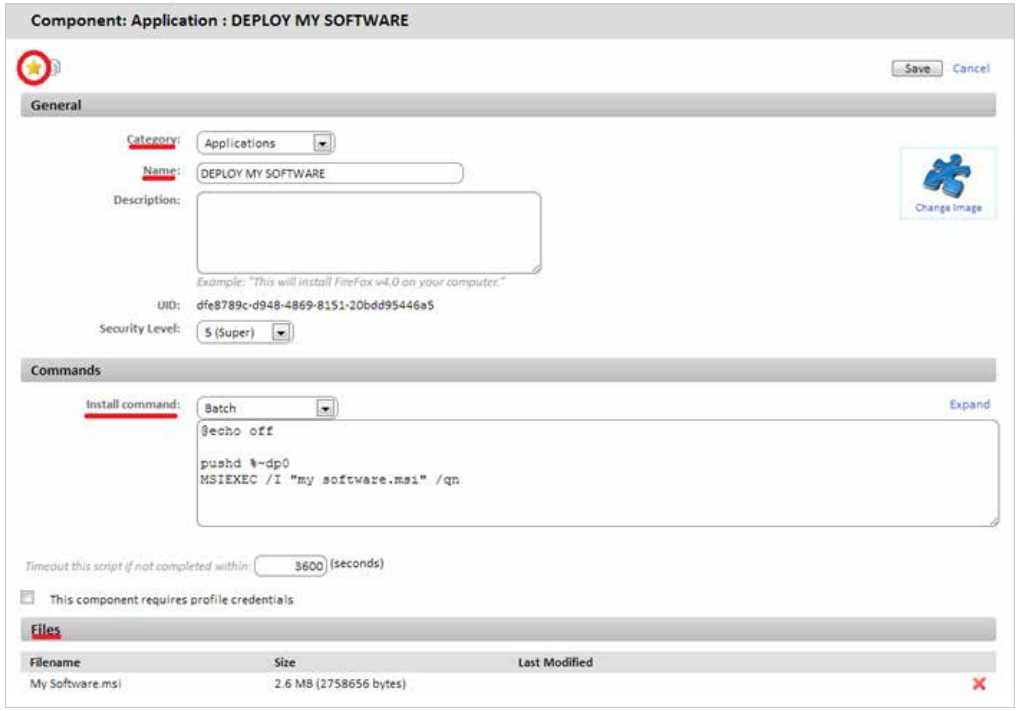
- ✔ Se añaden los ficheros y programas a instalar así como los accesos directos a crear. Esto se lleva a cabo en la pestaña Files and Folders.





- ✔ Finalmente se ejecuta Build con lo que el paquete MSI quedara generado en la carpeta de nuestra elección.

Una vez generado el paquete de instalación, los pasos para crear un componente de instalación y distribuirlo son equivalentes a ejemplos anteriores excepto por el script en Batch, que varía ligeramente en el comando para la instalación.



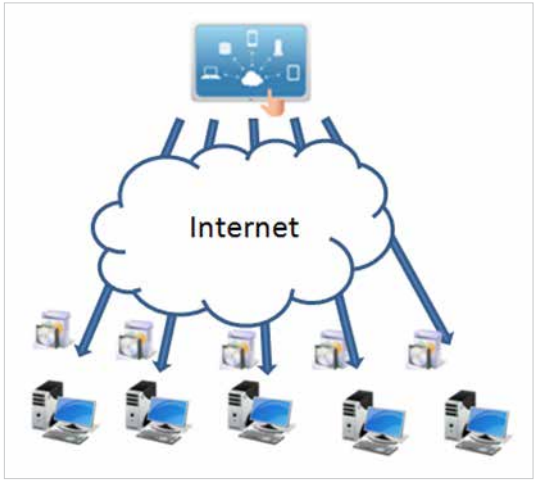
Se invoca a la utilidad MSIEXEC con el parámetro /qn para lanzar una instalación Silent.

- ✔ El componente es Favorito para que aparezca en los listados de componentes (icono de la estrella arriba a la izquierda) .
- ✔ La categoría (Applications) y el nombre del componente.
- ✔ El lenguaje de script utilizado (Install command), en este caso Batch.
- ✔ Agregar el paquete a instalar "My Software.msi".

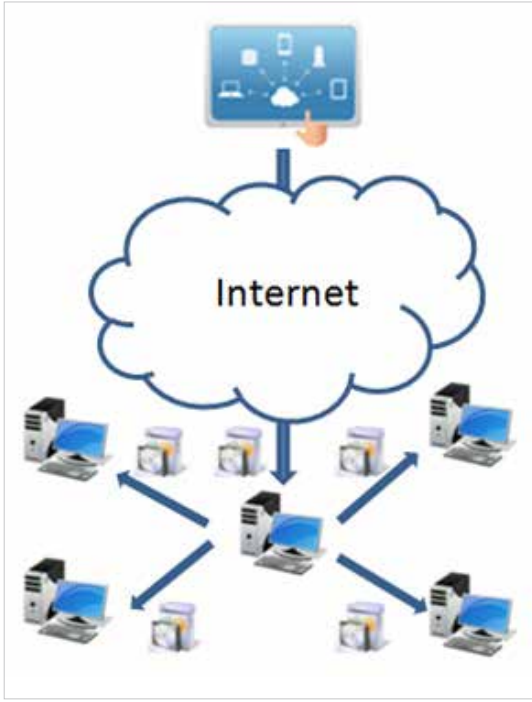
Ahorro de ancho de banda en el despliegue de software

El **Agente PCSM** instalado en cada uno de los dispositivos pregunta cada 60 segundos si hay alguna descarga que realizar desde el **Servidor PCSM** y en caso de ser así se ejecuta de forma individual para cada **Agente PCSM**. De esta forma para un paquete de instalación de 50 Mbytes y una red de 50 equipos el resultado aproximado de descarga será 2'4 Gbytes.

Para minimizar el volumen total de la descarga es posible promocionar uno de los dispositivos de la red al rol de repositorio / caché. De esta forma sólo este dispositivo realizará la descarga desde el **Servidor PCSM** para luego distribuir el paquete entre todos los dispositivos de la red afectados.



Para promocionar un dispositivo al rol de repositorio / caché deberá acceder al nivel Device del dispositivo en la Consola PCSM y hacer clic en el icono Add / Remove as local cache de la Barra de Acciones.



Desde ese momento, el dispositivo designado descargará y distribuirá los componentes y paquetes de instalación entre los dispositivos de la red local, acelerando el despliegue y minimizando el ancho de banda.

12. TICKETING

¿QUÉ ES EL SISTEMA DE TICKETING?

El incremento de equipos a gestionar y el creciente número de técnicos asignados a la resolución de problemas obliga más pronto que tarde a la implantación de un sistema que permita la documentación y coordinación de cada caso tratado por el departamento de IT.

Los sistemas de ticketing sirven para registrar cada incidencia desde el momento de su creación hasta su cierre, registrando todos los estados intermedios por el que evolucione.

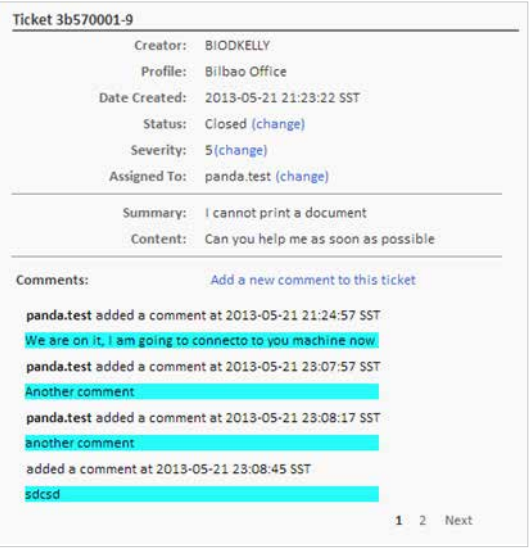
De esta manera es posible asignar un caso a un técnico concreto y reasignarlo a otro posteriormente si el técnico original ya no se encuentra disponible o la tarea requiere de conocimientos muy específicos, conservando toda la documentación y avances conseguidos hasta el momento y minimizando así las interrupciones al usuario final con requerimientos repetidos de información sobre el mismo problema.

Por otra parte, el hecho de obligar a documentar las incidencias permite reutilizar el procedimiento en el futuro y refinarlo, minimizando el tiempo de respuesta de los casos abiertos.

Finalmente con un sistema de ticketing es posible determinar la carga de trabajo del departamento de IT, filtrando los tickets que están abiertos en un determinado momento y asignar más recursos si fuera necesario.

DESCRIPCIÓN DE UN TICKET

Cada ticket contiene una serie de campos que lo describen:



- **Creator**: creador del ticket. Puede ser un dispositivo si el ticket fue creado desde el **Agente PCSM** por un usuario, o una cuenta del sistema si fue creado por un monitor y asignado a un técnico.
- **Profile**: agrupación de dispositivos a la que pertenece el ticket.
- **Date Created**: fecha de creación del ticket.
- **Status**: se distinguen cuatro estados:
  - **New**: ticket recién creado con la descripción del problema y asignado a un técnico. Todavía no se ha realizado ningún trabajo.
  - **In progress**: la incidencia está siendo gestionada por el técnico del departamento de IT asignado.
  - **Waiting**: la resolución de la incidencia se ha determinado por causas externas (falta de información, confirmación de cambios por parte del usuario u otras).
  - **Closed**: la incidencia se ha resuelto y se cierra.
- **Severity**: severidad del ticket. Si fue generado por un monitor se copia la severidad asignada a éste.
- **Assigned to**: técnico asignado para la resolución de la incidencia.
- **Summary**: resumen de la incidencia.
- **Content**: descripción de la incidencia.
- **Comments**: en este campo tanto el técnico como el usuario pueden añadir entradas que completen y actualicen la incidencia.

> Se recomienda utilizar el campo Comments frecuentemente, documentando los cambios de la incidencia y las acciones realizadas, tanto por parte del los técnicos del departamento de IT como del usuario con pruebas realizadas y otros datos de interés. El objetivo de esto es reutilizar esta información para agilizar futuras incidencias similares.

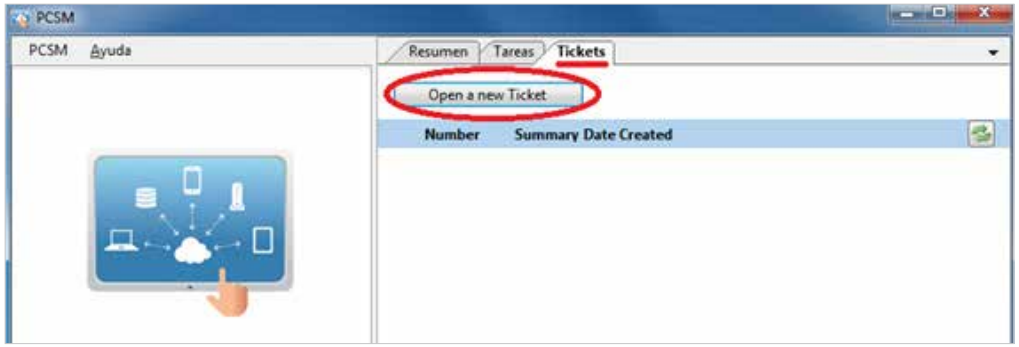
CREACIÓN DE UN TICKET

Los tickets son creados de tres maneras:

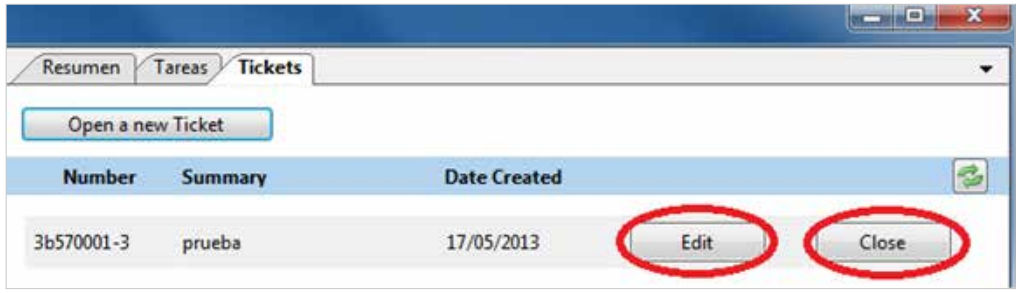
Manualmente por el usuario desde su propio Agente PCSM:

Si el usuario comprueba que su dispositivo funciona mal y quiere dejar constancia de los síntomas por escrito.

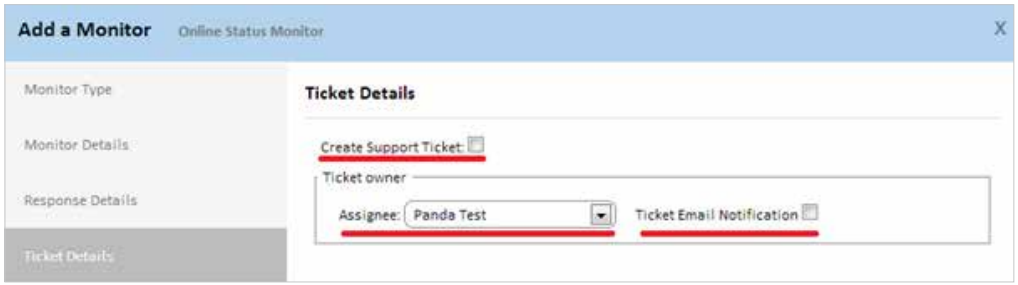
Para dar de alta un ticket de forma manual, el usuario tiene que abrir el **Agente PCSM** haciendo clic con el botón derecho sobre su icono seleccionando la opción Abrir y hacer clic en la pestaña Tickets, Open a New Ticket.



Una vez creado el ticket es posible añadir nuevos comentarios y cerrarlo.



De forma automática desde un monitor que detecte una condición definida como anómala en un dispositivo de usuario
Al definir una política de tipo Monitor, en la pestaña Ticket Details.



En este caso se puede elegir el técnico asignado y si se generará un mail de notificación con la creación del ticket.

De forma manual por departamento de IT desde la Consola PCSM: suelen ser recordatorios o tareas que entran de manera oficial en la cola del departamento.
Desde el Profile Level o System Level en la Barra de Pestañas, Support, haciendo clic en Create Support Ticket.

> Los tickets creados en el System Level no tienen Profile asignado y no se muestran en ninguno de los Profiles creados en la cuenta de **PCSM**.

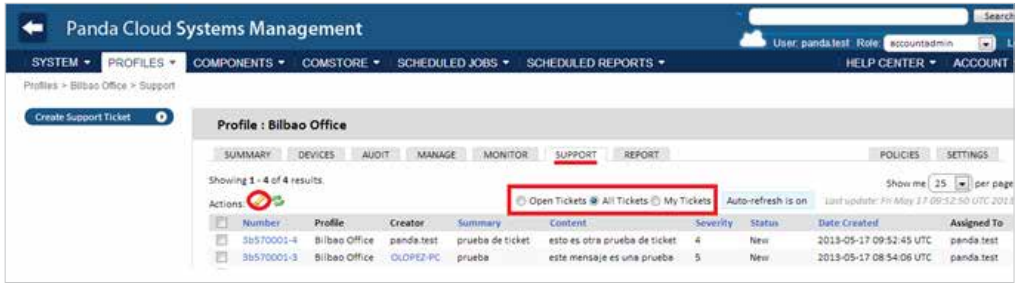
En este caso se pueden especificar la severidad del ticket y su contenido, así como asignarlo a un técnico para su resolución o reasignación posterior.

GESTIÓN DE TICKETS

La gestión de los tickets ya creados se realiza desde la Barra de Pestañas, Support en los niveles Profile, System o Device.

> Los tickets creados en los niveles inferiores se mostrarán en niveles superiores. Por ejemplo si se crean tickets en el Device Level aparecerán en el nivel Profile al que pertenezca ese dispositivo.

Con los iconos de la Barra de Acciones, podremos filtrar el listado de tickets (Open Tickets, My Tickets, All Tickets) o editar su estado con el icono del bolígrafo. Para cambiar la severidad, el estado y a quien está asignado se debe hacer clic en el número de ticket.



13. PATCH MANAGEMENT

¿QUÉ ES PATCH MANAGEMENT?

Patch Management es un conjunto de recursos orientadas a automatizar la distribución e instalación de parches y actualizaciones de software de forma centralizada.

Patch Management no solo facilita la actualización diaria del software de sus dispositivos sino que permite realizar auditorías, mostrando de forma sencilla y rápida aquellos equipos sin actualizar o con vulnerabilidades conocidas.

Con Patch Management el Administrador podrá reforzar la seguridad de la red y minimizar los fallos de software, garantizando que todos los dispositivos están actualizados con los últimos parches publicados.

Patch Management utiliza la API Windows Update existente en todos dispositivos Microsoft Windows compatibles con **Panda Cloud Systems Management**.

Patch Management es compatible con sistemas Microsoft Windows.

¿QUÉ PARCHES PUEDO DISTRIBUIR / APLICAR?

Todos los parches y actualizaciones publicadas por Microsoft a través de Windows Update pueden ser gestionados por **Panda Cloud Systems Management** de forma centralizada.

Microsoft publica actualizaciones para todos los sistemas operativos Windows que soporta en la actualizad y también para el software que desarrolla:

Microsoft Office	Visual Studio	Microsoft Lync
Exchange 2003	Zune Software	Silverlight
SQL Server	Virtual PC	Windows Media Player
Windows Live	Virtual Server	Otros…
Windows Defender	CAPICOM	

DISTRIBUCIÓN E INSTALACIÓN DE PARCHES

Panda Cloud Systems Management incorpora tres métodos complementarios para la gestión de parches, cada uno de ellos con diferentes funcionalidades para adaptarse a distintas necesidades y/o escenarios posibles.

Aunque los tres métodos son complementarios ciertas funcionalidades son compartidas por todos ellos. Si van a utilizarse varios métodos de gestión de parches de forma simultánea habrá que tener especial cuidado en no definir procedimientos que se solapen entre sí ya que el resultado final podrá variar según el orden definido, consiguiendo de esta forma resultados impredecibles.

Los procedimientos aquí descritos pueden colisionar con otros procedimientos definidos por software de terceros, como por ejemplo políticas de Windows Update definidas en una GPO. Se recomienda desactivar políticas de terceros fabricantes que interfieran con las definidas en **Panda Cloud Systems Management**.

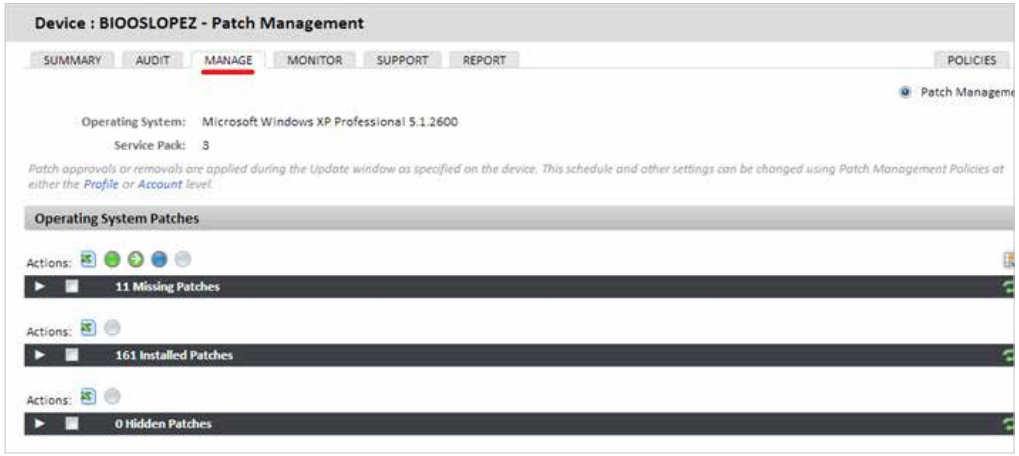
Método I: Gestión manual de parches

Descripción general.
La publicación manual de parches permite seleccionar uno por uno y de forma centralizada los parches a instalar, según el criterio que aplique el administrador.

Este método permite la máxima granularidad posible dado que en todo momento se muestran tanto los parches instalados en cada dispositivo como los pendientes de instalación.

Los niveles de agrupación compatibles con este método son los tres existentes: System Level, Profile Level y Device Level. De esta forma es posible seleccionar parches para un dispositivo en concreto (Device Level), para una agrupación concreta (Profile Level) o para todos los dispositivos dados de alta en **PCSM** (System Level).

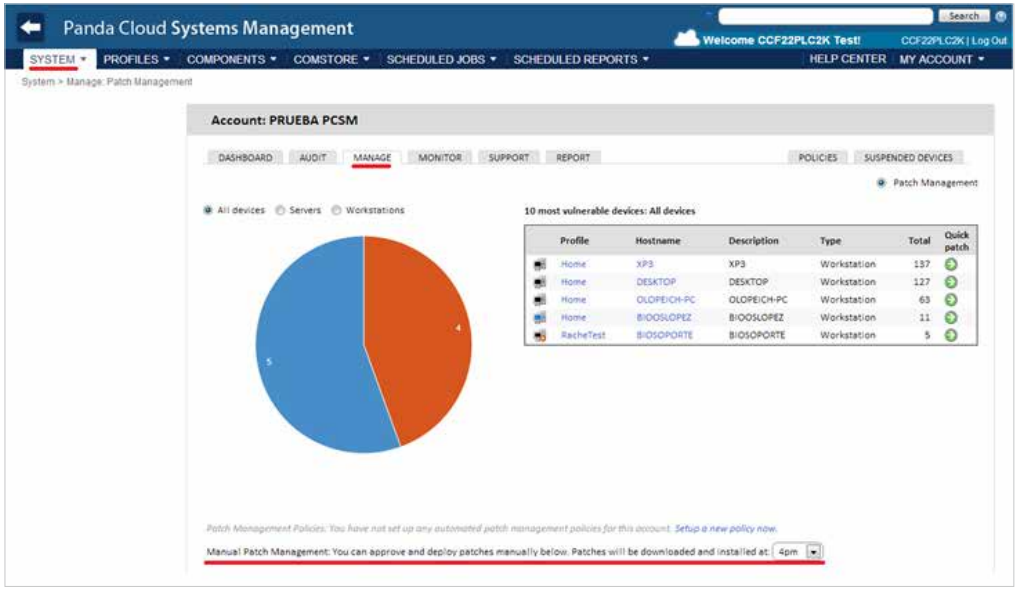
Acceso al método de gestión manual de parches.
Se accede a través de la Barra de Pestañas, Manage en los tres niveles disponibles.



Las acciones disponibles son:

- ✔ **Approve patch**: seleccionando los parches y haciendo clic en el icono del círculo verde.

Al aprobar una serie de parches éstos quedarán pendientes de instalación. La instalación de parches aprobados de forma manual se realiza en el momento definido en la Barra de pestañas, Manage del System Level.



Únicamente se puede definir en System Level el momento en que se instalarán los parches aprobados de forma manual. Todos los dispositivos gestionados por **PCSM** actualizarán los parches pendientes aprobados en el momento configurado.

- **Hide patch**: seleccionando los parches y haciendo clic en el icono del círculo azul para ocultarlos de los listados de parches disponibles.
- **Quick patch**: seleccionando los parches y haciendo clic en el icono del círculo verde con flecha los parches se instalarán de forma inmediata, sin esperar a momento definido en la configuración en Manage (System Level).
- **Reset patch**: haciendo clic en el icono del círculo blanco se limpia la selección de parches realizada.

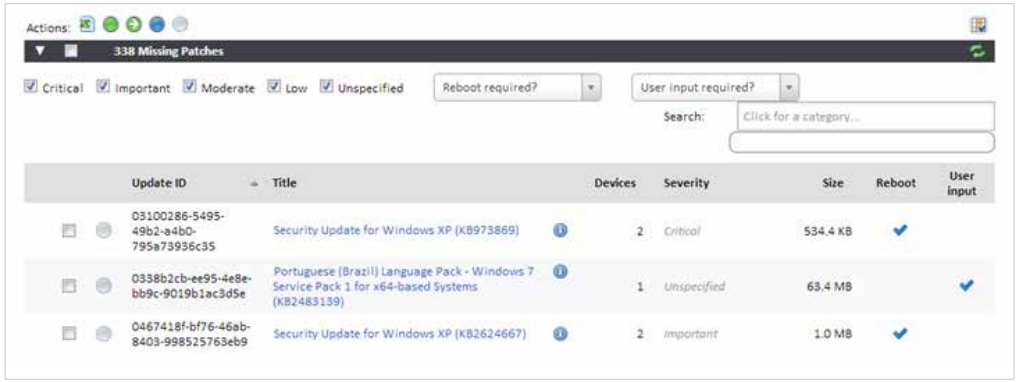
Visualización de parches

Todos los parches publicados por Microsoft a lo largo del tiempo se van agrupando en tres desplegables dependiendo de su estado con respecto al dispositivo administrado.

Los tres estados son:

- **Missing patches**: son los parches que todavía no han sido instalados en los dispositivos pertenecientes al nivel seleccionado. En el caso de niveles superiores a Device se muestra además el numero de dispositivos que no tienen instalado cada parche en concreto.
- **Installed Patches**: son los parches que ya han sido instalados en el nivel seleccionado. En el caso de niveles superiores a Device se muestra además el numero de dispositivos que tienen instalado cada parche en concreto.
- **Hidden Patches**: son los parches que el administrador ha decidido ocultar por no ser necesaria su aplicación ni recordatorio.

Con el objetivo de facilitar las búsquedas se tendrá acceso a información detallada al desplegar cada una de las categorías, así como a una Barra de Iconos para filtrar los listados de parches.



La Barra de Búsqueda permite elegir los parches mostrados según los siguientes criterios:

- **Severity**: es la severidad definida por Microsoft: Crítica, Importante, Moderada, Baja, Sin especificar.

Microsoft solo indica la severidad para los parches de seguridad (Security Updates). El resto de parches vienen generalmente con severidad "Sin Especificar".

- **Reboot required?** Si la aplicación del parche requiere reinicio del dispositivo.
- **User input required?** Si la aplicación del parche requiere interacción por parte del usuario.
- **Category:** permite buscar los parches que aplican a un software en particular.

Por cada entrada **PCSM** ofrece la información siguiente:

- **Check:** para seleccionar el parche.
- **Icono de acción:** los parches que tengan acciones pendientes aparecerán con el icono de la esfera en verde.
- **Titulo:** nombre completo del parche ofrecido por Windows Update.
- **Severidad:** importancia del parche ofrecida por Windows Update (solo para parches de seguridad Security Updates).
- **Size:** espacio que ocupa el parche en la descarga, ofrecida por Windows Update.
- **Reboot:** se indica si la instalación del parche requiere reinicio o no.
- **User input:** indica si la instalación del parche requiere interacción con el usuario o no (diálogos para aceptar EULAs y otros).

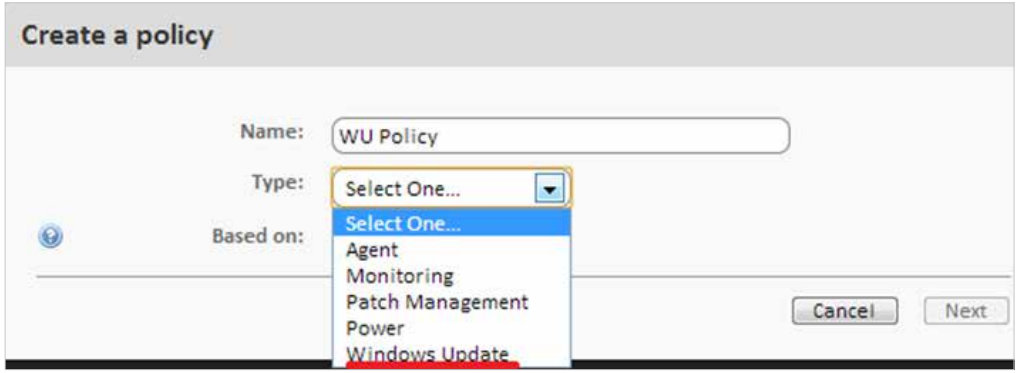
Escenarios de uso del método Gestión manual de parches.
Cuando el administrador requiera una supervisión muy precisa de los parches que se aplican en los dispositivos que administra.

Método II: Windows Update Policy

Descripción general
Las políticas de tipo Windows Update permiten configurar de forma centralizada las funcionalidades de Windows Update integradas en los dispositivos Windows de la red.

Al tratarse de una policy los niveles de agrupación compatibles con este método son System Level y Profile Level.

Acceso al método Windows Update Policy
Para acceder a este método hay que crear una política de tipo Windows Update en el Profile Level o System Level.



Se mostrará una pantalla donde se podrá configurar de forma centralizada el comportamiento de Windows Update de todos los dispositivos afectados por la política creada.

La configuración de las políticas Windows Update siguen el mismo esquema que los recursos Windows Update de cada dispositivo Windows individual.

Windows Update cataloga los parches que recibe en tres niveles:

- Importantes
- Recomendados
- Opcionales

Sólo los parches Importantes y Recomendados pueden ser instalados de forma automática. El resto de parches serán instalados de forma manual desde el propio dispositivo del usuario o sino desde **PCSM** utilizando otros métodos de Patch Management.

Toda la configuración de esta política es una transposición de las funcionalidades de Windows Update de los dispositivos Windows. Todas las acciones indicadas se refieren por tanto a los propios dispositivos y no al **Agente PCSM** o a la **Consola PCSM**.

Aunque la configuración de la política es única para todos los dispositivos, el comportamiento de Windows Update en cada dispositivo puede variar ligeramente entre las distintas versiones del sistema operativo.

A continuación se explican algunas opciones de la política:

- **Add target**: permite añadir filtros o grupos que delimiten el ámbito de aplicación de la política.
- **Patch Policy**: indica el comportamiento general de Windows Update dentro de cada dispositivo con respecto los parches catalogados como "Importantes" por Microsoft:

  Descarga e instalación automática.
  Descarga y selección manual por el usuario.
  Notificación sin descarga.
  Desactivar Windows Update.

- **Install new Updates**: indica en qué momento se instalarán los parches.
- **Give me recommended Updates the same way I receive important Updates**: aplica la política elegida en Patch Policy tanto a los parches Importantes como a los Recomendados.
- **Allow all users to install updates on the computer**: permite al usuario la instalación de parches de forma manual.
- **Give me updates for Microsoft products and check for new optional Microsoft software when updating Windows**: busca parches de tipo Opcional, generalmente parches de otros productos de Microsoft.
- **Show me detailed notifications when new Microsoft software is available**: le muestra al usuario notificaciones detalladas cuando se encuentre disponible nuevo software de Microsoft.
- **No auto-restart with logged on users for scheduled automatic updates installations**: si esta opción se activa los parches se aplican y se advierte al usuario que es necesario un reinicio. Si no se activa, el parche se instala y se advierte al usuario que se realizará un reinicio en 5 minutos.
- **Re-prompt for restart with scheduled installations**: establece el tiempo para que Windows Update vuelva a solicitar al usuario el reinicio del dispositivo en caso de que haya parches instalados que lo requieran.
- **Delay restart for scheduled installations**: establece el tiempo que el sistema espera para reiniciar después de instalar los parches. Si no se indica nada se toma el valor por defecto: 15 minutos.
- **WSUS**: permite utilizar un servidor Windows Server Update Services alternativo local o remoto para minimizar la descarga de parches individuales por cada dispositivo en la red.
- **Enable Client-side targeting**: en caso de utilizar un servidor WSUS con Client-side targeting activado, los grupos y los dispositivos que los forman son definidos de forma manual en el servidor WSUS. En este parámetro de la política se permite especificar los grupos separados por punto y coma a los que pertenece el dispositivo sobre el que aplica la política.

Si algún o todos los dispositivos afectados por la política Windows Update no coinciden con los dispositivos definidos en los grupos de WSUS, la política quedará sin efecto en esos dispositivos.

Escenarios de uso del método Windows Update Policy.

- Cuando el administrador requiere la garantía de que todos los parches importantes son instalados en todos los dispositivos de la red de forma automática, sin posibilidad de que el usuario entorpezca el proceso.
- Cuando el administrador no requiere un control individual de cada uno de los parches que se instalan y puede delegar en Microsoft la decisión de instalación según su catalogación de los parches en Importantes o Recomendados.
- Cuando no se requiere la instalación automática de los parches catalogados como Opcionales.

Metodo III: Patch Management Policy

Descripción general
Las políticas de tipo Patch Management permiten la instalación de parches de forma automática, de forma similar a las políticas de Windows Update.

La principal diferencia viene de forma de agrupar los parches a instalar. Si en el método Manual se permitía elegir de forma individual cada uno de los parches a aplicar y en el método Windows Update Policy se permitía aplicar parches por niveles (Importante, Recomendado, Opcional), Patch Management Policy permite seleccionar los parches a aplicar agrupándolos de forma más flexible: por nombre, descripción, tamaño, tipo y otros.

Al tratarse de una policy los niveles de agrupación compatibles con este método son System Level y Profile Level.

Acceso al método Patch Management Policy
Para acceder a este método hay que crear una política de tipo Patch Management Policy al nivel Profile o System.

Se mostrará una pantalla donde se podrá configurar de forma centralizada el comportamiento de Patch Management para todos los dispositivos afectados por la política creada.

A continuación se explican las opciones de la política menos evidentes:

- **Add target**: permite añadir filtros o grupos que delimiten el ámbito de aplicación de la política.
- **Window**: permite definir una ventana de instalación de parches. Durante la ventana de instalación la descarga de parches puede realizarse de forma distribuida para no colapsar puntualmente la línea de datos del clienteactivando el check "Randomize the start time to smooth network load".
- **Install criteria**: permite instalar todos los parches publicados de forma indiscriminada que afecten al dispositivo (Install all patches) o establecer un filtro que cumpla con uno o varios criterios. Para establecer un criterio:
  - Elegir un campo de la información publicada asociada a cada parche sobre el cual se realizará el filtrado (Field).
  - Elegir la condición (Condition). Varía según el tipo de datos del Field elegido.
  - Elegir el término de búsqueda (Search term). Varía según el tipo de datos del Field elegido.

Escenarios de uso del método Patch Management Policy.

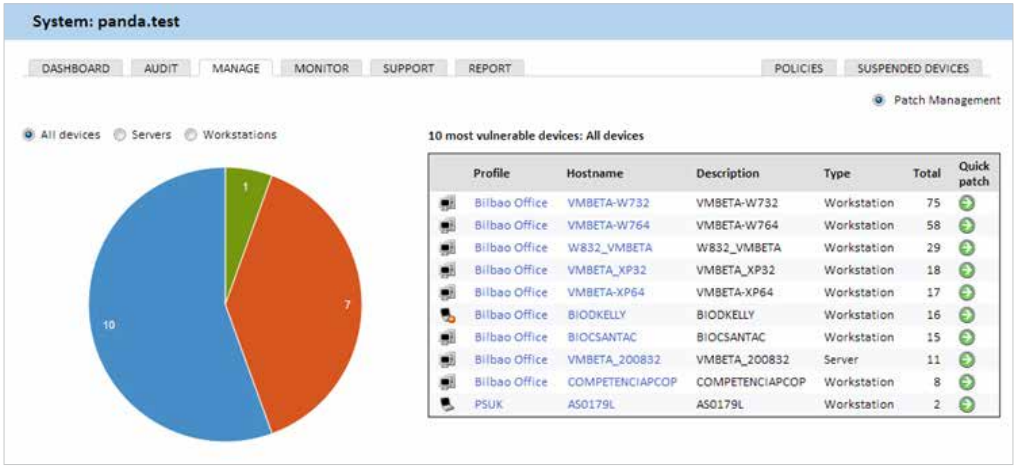
- Cuando el administrador necesita más granularidad que la aportada por el método Windows Update Policy.
- Cuando el administrador requiere instalar todos los parches sin excepción, de forma automática y centralizada.

Tabla comparativa de métodos

Método	Granularidad selección parches	Automatización	Tiempo de configuración
Gestión manual	**Alta** Selección parche por parche.	**Baja** Requiere de la aprobación manual y continua de parches.	**Alto** Revisión manual de todos los parches publicados y selección.
Windows Update Policy	**Baja** Selección de parches según grupos "Importantes" y "Recomendados".	**Alta** Se configura una vez los grupos de parches a instalar.	**Bajo** Elegir si instalar los parches "importantes" y "opcionales".
Patch Management	**Media** Selección de parches por múltiples criterios configurables.	**Alta** Una vez creados los filtros los parches se instalan automáticamente según Microsoft los libere.	**Medio** Establecer los filtros para seleccionar los parches a instalar.

AUDITORÍAS

En la pestaña Manage del Profile Level o System Level se muestra de un solo vistazo el estado del parque informático administrado en lo que a instalación y aplicación de parches se refiere.



Criterio de selección

El criterio de selección (All devices, Servers, Workstations) establece un filtrado previo para todos los dispositivos del profile (Manage en Profile Level) o de todos los dispositivos administrados en su conjunto (Manage en System Level).

Gráfico de tarta

Una vez establecido el criterio de filtrado el gráfico de tarta mostrará:

- Número de dispositivos con actualizaciones no criticas sin instalar (azul).
- Número de dispositivos con actualizaciones criticas sin instalar (naranja).
- Número de dispositivos actualizados de forma completa (verde).

Listado de equipos vulnerables

Haciendo clic en cualquiera de las dos secciones del gráfico de tarta se actualiza el listado de equipos vulnerables.

El listado de equipos vulnerables muestra información relativa a los dispositivos más vulnerables (actualizaciones críticas o actualizaciones no críticas sin aplicar). Además ofrece varios accesos directos para solucionar esta situación:

- **Hostname**: permite entrar al Device Level para ese dispositivo en particular, con el objeto de ver qué parches no han sido aplicados exactamente y aprobar los que sean necesarios.
- **Quick Patch**: aplica de forma inmediata los parches indicados por el criterio de selección: críticos o no críticos según hayamos hecho clic en la zona azul o naranja de la gráfica de tarta.

14. CUENTAS DE USUARIO Y ROLES

¿QUÉ ES UNA CUENTA DE USUARIO?

Una cuenta de usuario es una colección de información incluyendo credenciales de acceso a la **Consola PCSM** y al **Agente PCSM**, necesarias para administrar los dispositivos de una red.

Las cuentas de usuario son utilizadas únicamente por Administradores de IT que quieran utilizar los servicios ofrecidos por **Panda Cloud Systems Management**.

Generalmente cada administrador de IT tiene una única cuenta de usuario.

Los usuarios de dispositivos no necesitan ningún tipo de cuenta de usuario ya que no acceden a la **Consola PCSM** y el **Agente PCSM** instalado en sus dispositivos está por defecto configurado en Modo Monitor.

A diferencia del resto del manual donde "usuario" es la persona que utiliza un dispositivo gestionado por un administrador con la ayuda de **Panda Cloud Systems Management**, en este capítulo "usuario" puede referirse a una cuenta de usuario o cuenta de acceso a la **Consola PCSM**.

¿QUÉ ES UN ROL?

Un rol es una configuración específica de permisos de acceso a la **Consola PCSM**, que se aplica a una o más cuentas de usuario. De esta forma un administrador concreto estará autorizado a ver o modificar determinados recursos de la **Consola PCSM** según el rol al que pertenezca la cuenta de usuario con la que acceda a **Panda Cloud Systems Management**.

Una o más cuentas de usuario pueden pertenecer a uno o más roles.

Los roles solo afectan al nivel de acceso de los administradores de IT a los recursos de la **Consola PCSM** para gestionar los dispositivos de la red. No afectan al resto de usuarios de dispositivos.

¿PORQUE SON NECESARIOS LOS ROLES?

En un departamento de IT pequeño todos los técnicos van a acceder a la Consola PCSM como administradores sin ningún tipo de límite; sin embargo, en departamentos de IT de mediano o gran tamaño o en partners con muchos clientes es posible que sea necesario segmentar el acceso a los dispositivos aplicando tres criterios:

- **Según la cantidad de dispositivos a administrar**.
  Redes de tamaño medio / grande o redes pertenecientes a delegaciones de una misma empresa o a distintos clientes de un mismo partner pueden requerir de la distribución y asignación de dispositivos a técnicos. De esta forma, los dispositivos de una delegación administrados por un técnico determinado serán invisibles para los técnicos que administren los dispositivos de otras delegaciones.

  También pueden existir restricciones de acceso a datos delicados de clientes concretos que requieran un control exacto de los técnicos que van a poder manipular los dispositivos que los contienen.

- **Según el cometido del dispositivo a administrar**.
  Según la función que desempeñe un dispositivo puede asignarse a un técnico experto en ese campo: por ejemplo los servidores de bases de datos de un cliente o de todos los clientes gestionados por el partner pueden ser asignados a un grupo de técnicos especialistas, y de esa misma forma otros servicios como por ejemplo servidores de correo podrían no ser visibles para este grupo.

- **Según los conocimientos del técnico**.
  Según las capacidades del técnico o su función dentro del departamento de IT puede requerirse únicamente un acceso de monitorización / validación (solo lectura) o por el contrario uno más avanzado, como el de modificación de configuraciones de dispositivos.

Los tres criterios se pueden solapar dando lugar a una matriz de configuraciones muy potente y fácil de establecer y mantener, que permite delimitar perfectamente las funciones de la Consola PCSM accesibles a cada técnico, según su perfil y responsabilidades.

EL ROL ACCOUNTADMIN

Una licencia de uso de **Panda Cloud Office Protection** viene con un rol de control total predefinido, llamado accountadmin. A este rol pertenece la cuenta de administración creada por defecto y con ella es posible realizar absolutamente todas las acciones disponibles en la **Consola PCSM**. Accountadmin además es el único rol que puede crear nuevos roles y usuarios, así como modificar los ya existentes.

El rol accountadmin no puede borrarse del **Servidor PCSM** y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la **Consola PCSM**.

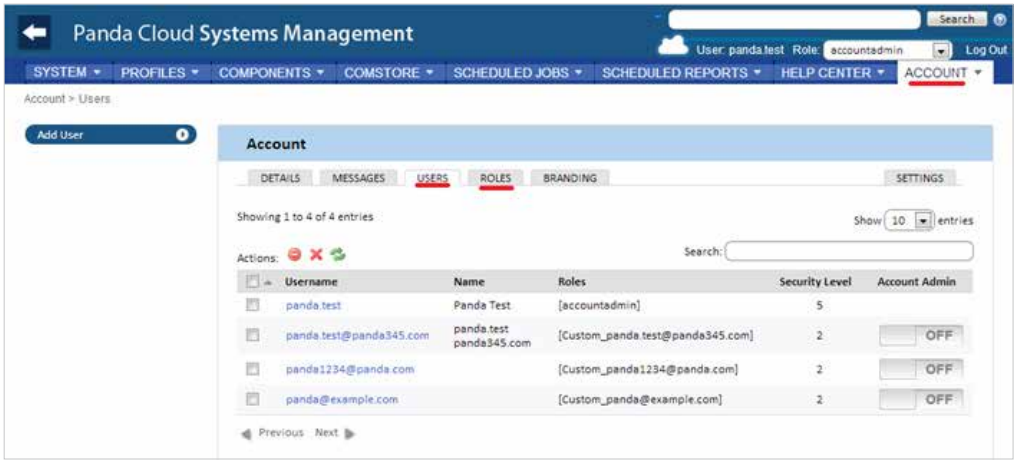
Todos los procedimientos descritos en este capítulo requieren de una cuenta que pertenezca al rol accountadmin.

ACCESO A LA CONFIGURACIÓN DE CUENTAS DE USUARIOS Y ROLES

En el Menú General, Account aparecen dos entradas asociadas a la gestión de roles y cuentas usuario:

- **Usuarios**: permite crear nuevas cuentas de usuario y definir su pertenencia a uno o varios roles.

- **Roles**: permite crear y modificar una nueva configuración de acceso a los recursos de **Panda Cloud Systems Management**.



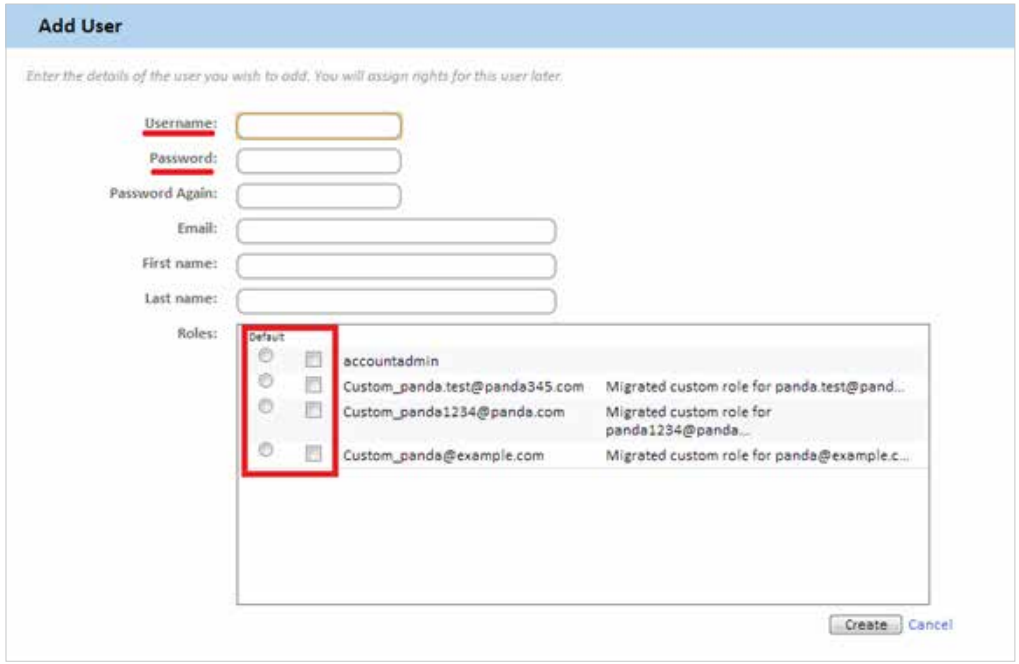
Las pestañas de usuarios y roles solo son accesibles si el usuario pertenece al rol especial accountadmin.

CREACIÓN Y CONFIGURACIÓN DE CUENTAS DE USUARIO

En el Menú General Account, Users podremos realizar todas las acciones necesarias relativas a la creación y modificación de cuentas de usuario.

1) Añadir nueva cuenta de usuario: haciendo clic en Add user se permitirá añadir un nuevo usuario, establecer su contraseña, indicar el rol o roles a los que pertenece y establecer su nivel de seguridad asociado (de 1 a 5).

El nivel de seguridad asociado al usuario permite restringir el acceso a aquellos componentes desarrollados o importados de la ComStore cuyo nivel de seguridad sea superior.



2) Editar una cuenta de usuario: haciendo clic en el nombre del usuario se mostrará un formulario con todos los datos de la cuenta.

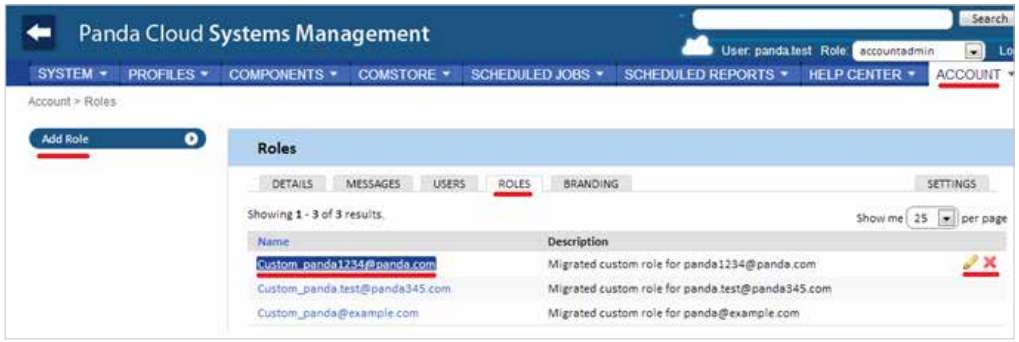
3) Borrar o desactivar cuentas de usuarios: seleccionando los usuarios marcando los checkbox asociados y haciendo clic en los iconos de prohibido y aspa de la Barra de Acciones.

4) Dar permisos de control total: pulsando el botón On/OFF en Account Admin.

Una cuenta de usuario puede pertenecer a un único rol o a más de uno. En este último caso en la **Consola PCSM** se mostrará un desplegable mediante el cual es posible elegir el rol con el que la cuenta de usuario opera.

CREACIÓN Y CONFIGURACIÓN DE ROLES

En el Menú General Account, Roles, podremos realizar todas las acciones necesarias relativas a la creación y modificación de roles.



5) Añadir nuevo rol: haciendo clic en Add Role se permitirá añadir un nuevo rol. Se nos preguntará por su nombre y si se quiere tomar como base una configuración / plantilla vacía o el nuevo rol se basa en uno anterior.

6) Editar un rol: haciendo clic en el nombre del rol o en el icono del lápiz se mostrará un formulario con todas sus configuraciones.

7) Borrar rol: con el icono de la X se borrará el rol seleccionado.

Si al borrar un rol tiene cuentas de usuario asignadas se nos preguntará qué nuevo rol será asignado a esas cuentas.

CONFIGURACIÓN DE ROLES

La configuración de un rol se divide en 4 apartados:

- **Device visibility**: habilita o restringe el acceso a agrupaciones de dispositivos.
- **Permissions**: habilita o restringe el acceso a funcionalidades de la Consola PCSM.
- **Agent Browser Tools**: habilita o restringe el acceso a funcionalidades en el Agente PCSM.
- **Membership**: indica las cuentas de usuario que pertenecen al rol configurado.

Device Visibility

Con este grupo de configuración se puede indicar qué dispositivos de la red serán visibles para los usuarios de la Consola PCSM que pertenezcan a un rol determinado.

Es posible establecer el acceso a las cuatro agrupaciones estáticas disponibles en PCSM:

- Profiles
- System Device Groups
- Profile Device Groups
- System Profile Groups

> No es posible establecer el acceso a agrupaciones dinámicas como filtros.

Cada una de ellas permite establecer si las agrupaciones de dispositivos del tipo indicado y creadas previamente por un administrador estarán accesibles o no en un rol determinado.

Pulsando en el botón ON se muestra un panel de configuración.

Un grupo listado en el Textbox Include será visible para todas las cuentas de usuario que pertenezcan a ese rol. De la misma forma si el grupo está listado en el Textbox Exclude ese grupo de dispositivos no será visible en la **Consola PCSM**.

Permissions

Permissions establece el nivel de acceso para cada una de las pestañas principales de la Consola PCSM:

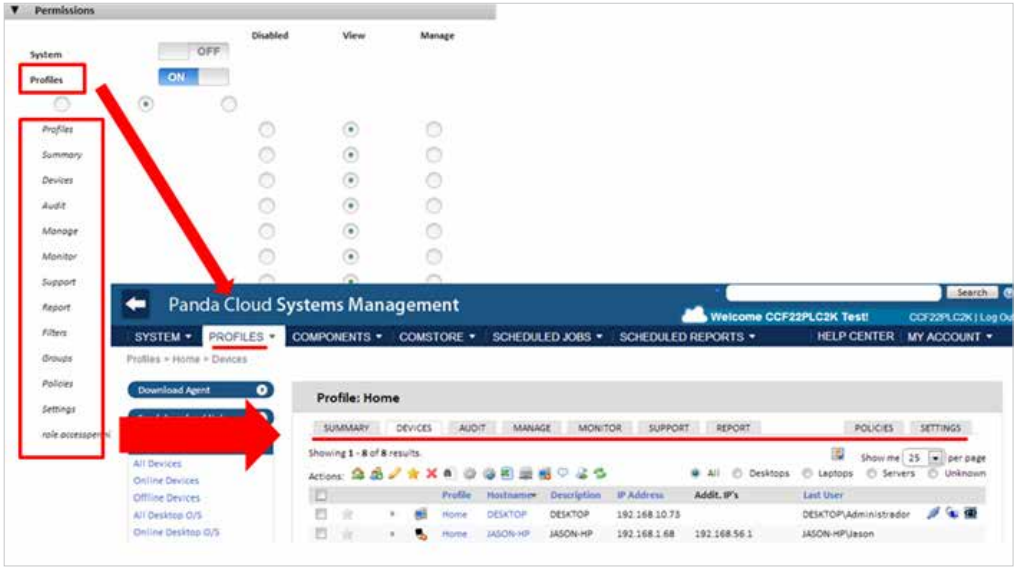
- System
- ComStore
- Account
- Profiles
- Jobs
- Components
- Reports

Los niveles de acceso son tres:

- Disabled
- View
- Manage

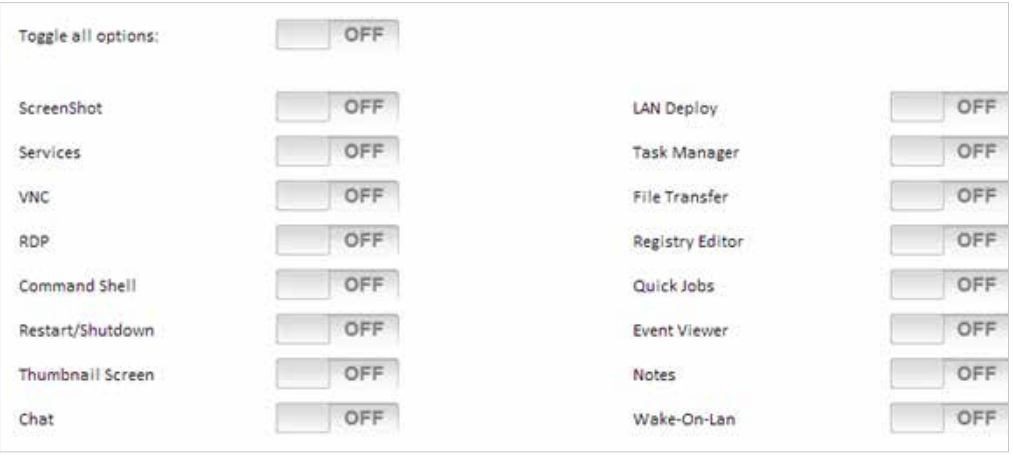
Pulsando el botón ON se puede definir cada una de las categorías de forma independiente. El contenido de cada categoría en el apartado Permissions es una transposición de las opciones que se muestran en la **Consola PCSM** más el nivel de acceso, definible para cada una de las opciones.

Haciendo clic en el Menú General, Profiles por ejemplo podemos comprobar la equivalencia de pestañas en la **Consola PCSM**.



Agent Browser Tools

Con este grupo de configuración se permite especificar el acceso a las diferentes herramientas de administración remota disponibles en el **Agente PCSM**.



Cualquier cambio realizado en Agent Browser Tools debe de ir acompañado de un reinicio del **Agente PCSM**.

Estas restricciones aplican a la **Consola PCSM** local del **Agente PCSM**, al iniciar sesión para administración dispositivos remotos (Modo Administrador).

Membership

Permite configurar las cuentas de usuario que pertenecen al rol configurado.

¿CUÁNTOS ROLES DIFERENTES SON NECESARIOS?

Es posible generar tantos roles como se consideren necesarios teniendo en cuenta que el objetivo final de un rol es el de limitar el acceso de los administradores a dispositivos o a recursos de la **Consola PCSM** para aportar así una mayor seguridad y protección contra el fallo humano. Sin embargo esta mayor seguridad viene de la mano de una menor flexibilidad a la hora de reutilizar el personal técnico entre varios clientes o tareas, de modo que el número exacto de roles en un sistema lo dará la ponderación que se haga de estas dos variables: flexibilidad vs seguridad.

Roles horizontales

De una forma general una empresa con varias delegaciones y un equipo de IT independiente por cada delegación buscará un rol de control total pero limitado a los dispositivos de cada delegación.

De esta forma los dispositivos administrados por la delegación A no serán visibles por la delegación B y viceversa.

En una empresa con varias delegaciones será necesaria la siguiente configuración por cada delegación:

- ✔ 1 Profile o System Group que agrupe a los dispositivos de la delegación.
- ✔ 1 rol que permita el acceso a los dispositivos del Profile y deniegue el resto.
- ✔ Una cuenta por cada técnico, asignada al rol que cubra la delegación designada.

El mismo esquema se puede utilizar para el partner que quiera segregar clientes y asignarlos a técnicos concretos.

Roles verticales

Para dispositivos fuertemente orientados a tareas especificas, como pueden ser servidores de impresión, base de datos, correo, etc. pueden crearse roles que limiten el acceso a este tipo de dispositivo.

De esta forma una empresa o partner que tenga múltiples delegaciones o clientes con servidores de correo puede querer agruparlos y asignarlos a un grupo de técnicos para su administración, mientras el resto de técnicos de perfil más generalista se dedican a mantener los dispositivos de usuario.

Será necesaria la siguiente configuración general:

- ✔ Un System Group que agrupe a todos los servidores de correo independientemente del Profile / cliente/ delegación al que pertenezcan.
- ✔ Un rol A que permita el acceso a los dispositivos contenidos en el System Group y deniegue el acceso al resto de dispositivos.
- ✔ Un rol B que deniegue el acceso a los dispositivos contenidos en el System Group y permita el acceso al resto de dispositivos.
- ✔ Tantas cuentas de usuario del rol A como técnicos lleven el mantenimiento de los servidores de correo de la empresa o partner.
- ✔ Tantas cuentas de usuario del rol B como técnicos lleven el mantenimiento de los dispositivos de usuario de la empresa o partner.

Roles de acceso a recursos

Atendiendo al perfil o grado de experiencia de cada técnico, el director del departamento de informática puede dividir el trabajo de los miembros de su departamento. De esta forma es posible crear grupos de técnicos con responsabilidades complementarias:

- ✔ Técnicos de monitorización y generación de informes: con acceso completo a la Barra de pestañas, Reports y acceso de solo lectura al resto de la **Consola PCSM**.
- ✔ Técnicos de desarrollo de scripts y deploy de software: con acceso al Menú General, componentes y ComStore.
- ✔ Técnicos de soporte: con acceso a la Barra de Pestañas, Support y a los recursos del dispositivo del usuario a través del **Agente PCSM**.

También es posible limitar el acceso a determinados componentes de la ComStore o desarrollados por el departamento de IT que realicen operaciones delicadas en los dispositivos del usuario, asignando niveles de seguridad superiores al establecido en la cuenta de usuario.

15. GESTIÓN DE DISPOSITIVOS MÓVILES

Panda Cloud Systems Management incluye herramientas de **MDM** (Mobile Device Management) que le permiten gestionar el parque de dispositivos móviles de la empresa de una forma sencilla y centralizada. Con **PCSM** podrá hacer frente a la creciente presencia de dispositivos móviles en su empresa desde la misma consola que ahora utiliza para gestionar el resto de su parque informático.

¿QUÉ PLATAFORMAS SE SOPORTAN?

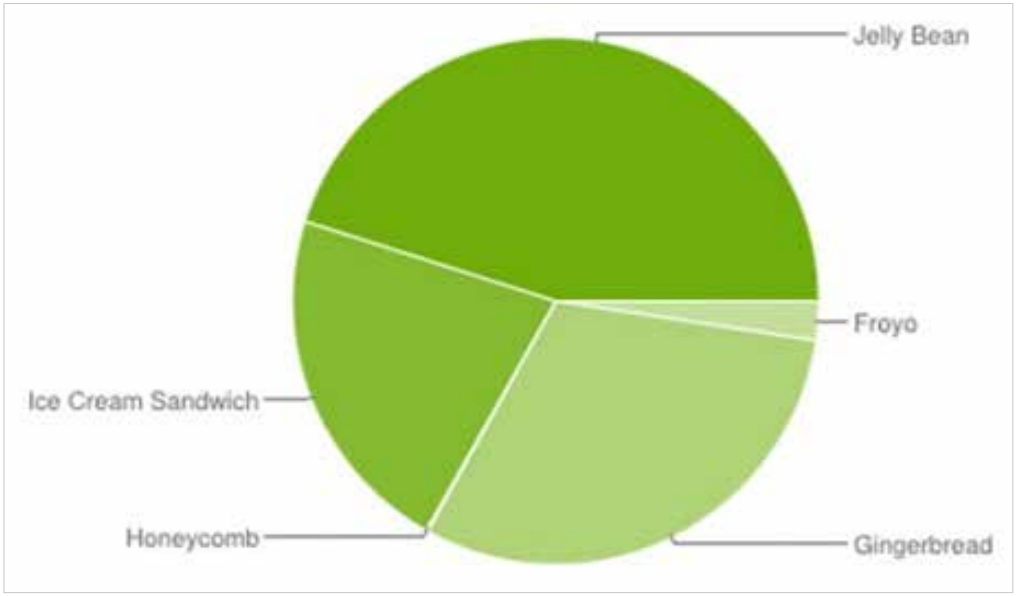
Panda Cloud Systems Management es compatible con tablets y smartphones iOS y Android.

Los terminales iPhone y tablets iPad que soporten iOS 6 o superior son compatibles. A continuación se ofrece un listado orientativo:

Modelo		
iPhone 3G (*)	iPhone 4 (*)	iPhone 4S (*)
iPhone 5	iPhone 5C	iPhone 5S
iPad 2 (*)	iPad (3° generación) (*)	iPad (4° generación)
iPad Mini		

(*) Requiere actualización a iOS 6 o superior para ser compatible.

Los terminales Android compatibles son todos aquellos que soporten la versión 2.3.3 (Gingerbread) y superiores, en la actualidad la práctica totalidad de los terminales en circulación exceptuando un porcentaje residual que aún funcionan con Froyo (2.2.x).

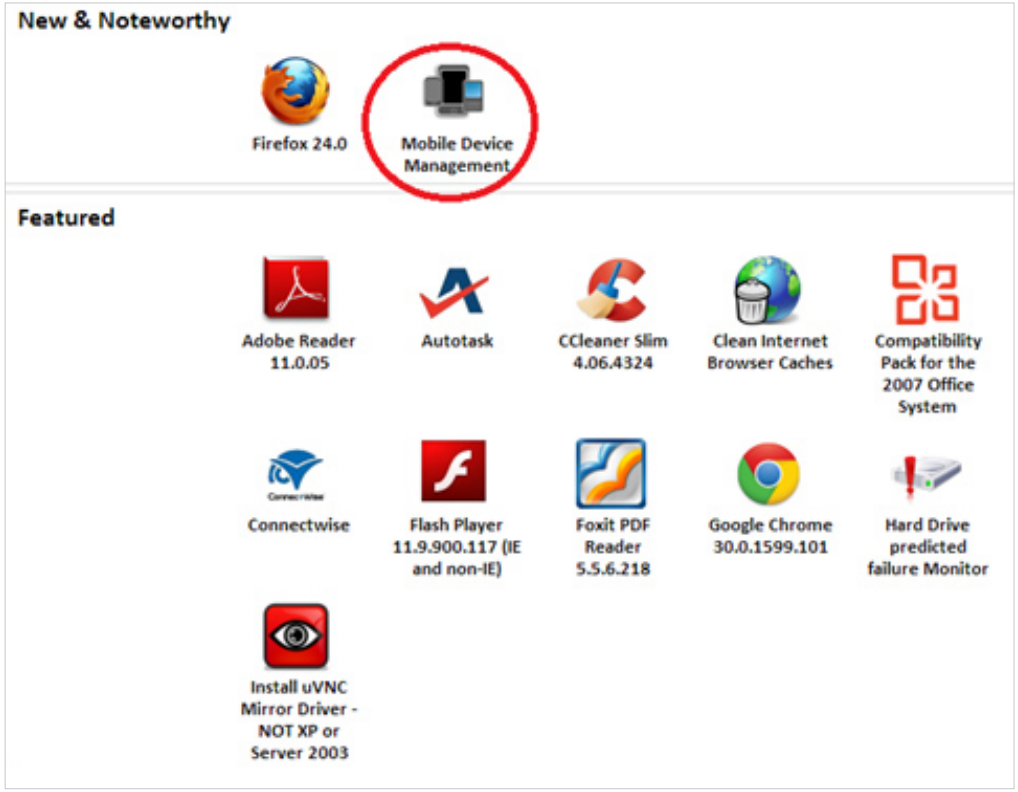


INTEGRACIÓN DE DISPOSITIVOS MÓVILES EN PCSM

Para poder administrar dispositivos móviles desde la consola centralizada se han de seguir los pasos descritos a continuación.

Activación de las funcionalidades MDM de la consola

Para poder interactuar con los dispositivos móviles desde la consola es necesario habilitar las funcionalidades MDM. Esto se consigue importando el componente gratuito "Mobile Device Management" directamente desde la Comstore.

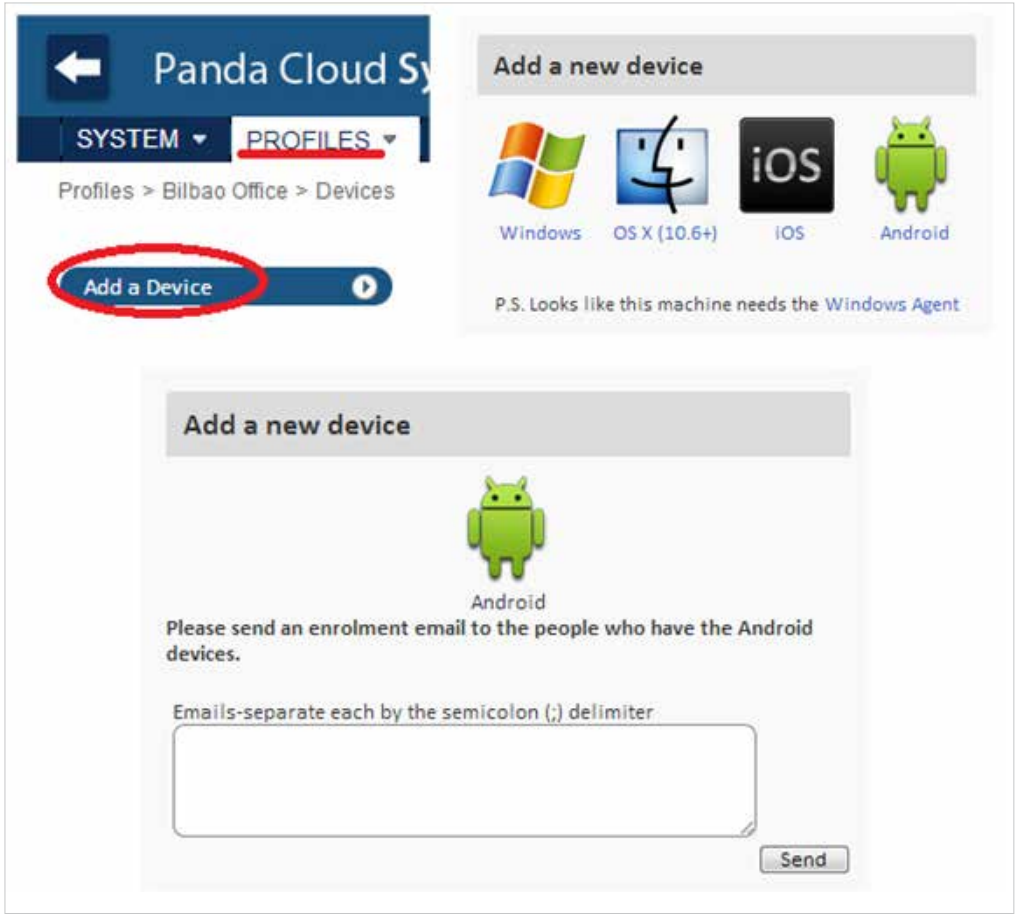


Aunque el componente "Mobile Device Management" se ofrece sin cargo extra cada dispositivo móvil con un **Agente PCSM** instalado contará como una licencia de dispositivo normal a los efectos del cómputo global de licencias adquiridas.

Instalación del agente

Al igual que con el resto de dispositivos, para poder administrar un móvil o tablet compatible es necesario instalar un **Agente PCSM** en el dispositivo que permita la comunicación segura con el **servidor PCSM**.

Para enviar el **Agente PCSM** al dispositivo del usuario **Panda Cloud Systems Management** creará un correo electrónico con toda la información necesaria. Para ello hay que seleccionar el Profile al que pertenecerá el dispositivo móvil y añadir un dispositivo de tipo Android o iOS, indicando la dirección de correo del usuario.

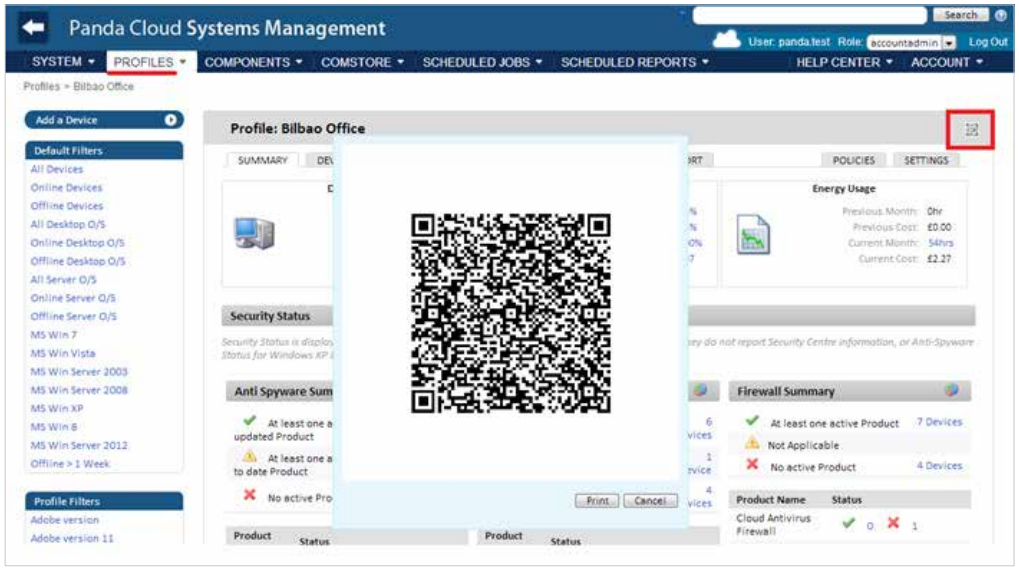


El cliente recibirá un correo con un link de descarga directa desde la Apple Store o Google Play y un fichero .MDM que es el que contiene la información del Profile al que quedará asociado el dispositivo.

Asociación del dispositivo al Profile

Los **Agentes PCSM** de iOS y Android ya instalados en el dispositivo del cliente necesitan de un proceso manual que los vincule con el Profile elegido. El proceso de vinculación se puede realizar de dos formas:

- **Opción 1**: Capturando el código QR con la cámara del dispositivo.



En el dispositivo móvil del usuario tocar el icono de la rueda para lanzar la cámara y enfocarla hacia el código QR de la pantalla.

Una vez interpretado el código el **Agente PCSM** mostrara el mensaje "Connected" en el dispositivo del usuario y se mostrará en la **Consola PCSM**.

- **Opción 2**: Importando en el agente el fichero .MDM enviado en el mensaje de correo.

En los móviles que no incorporen cámara es posible abrir el fichero .MDM desde el propio mensaje de correo, tocando simplemente el fichero.

Una vez cargado el fichero .MDM el **Agente PCSM** mostrara el mensaje "Connected" en el dispositivo del usuario y se mostrará en la **Consola PCSM**.

Solo se soporta la importación del fichero MDM desde el cliente de correo nativo del terminal.

Importación del certificado en la Consola PCSM para dispositivos basados en iOS

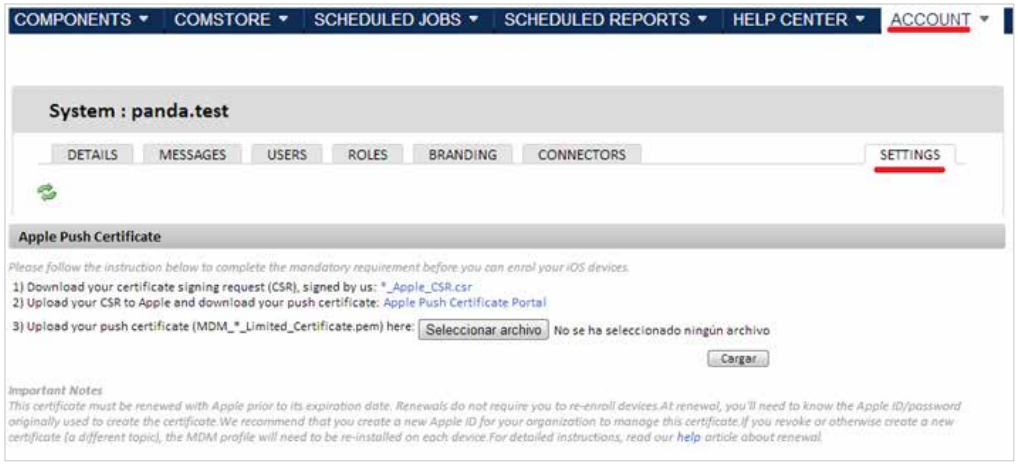
Además de los apartados anteriores es necesario incorporar en la **Consola PCSM** el certificado generado por Apple para que los dispositivos iOS puedan conectar con el **Servidor PCSM**.

La importación del certificado de Apple es un proceso de obligado cumplimiento una sola vez por cada Cliente / Partner que vaya a administrar uno o más dispositivos de usuario basados en iOS.

La instalación del certificado es un requisito impuesto por Apple para garantizar la integridad, autenticidad y confidencialidad de las comunicaciones entre el **Servidor PCSM** y el dispositivo de usuario.

Para ello hay que seguir los siguientes pasos:

- ✔ En el menú Account, Settings al final de la página se muestra la configuración de certificados para Apple.



- ✔ Exportar la petición de firma de certificado (CSR) firmado por Panda Security (*_Apple_CSR.csr)

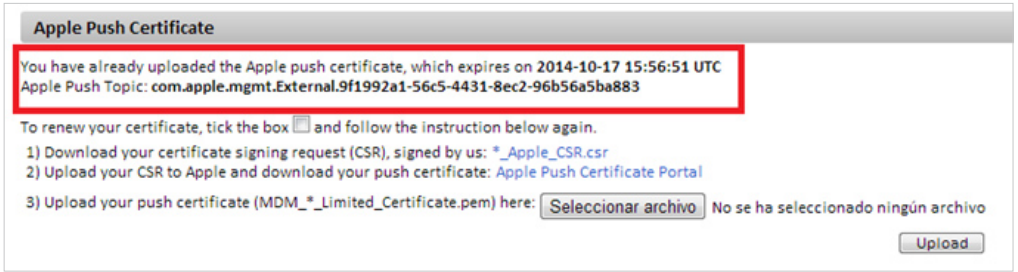
- ✔ Importar el fichero CSR en el portal Apple Push Certificate Portal.

Para acceder al portal Apple Push Certificate Portal es necesario disponer de una cuenta de Apple. Cualquier cuenta de iTunes será suficiente pero si quiere crear un nuevo juego de credenciales visite *https://appleid.apple.com/,* haga clic en "Crea un ID de Apple" y siga las instrucciones en pantalla.

Con las credenciales preparadas visite la página *https://identity.apple.com/pushcert*, clique en "Create Certificate" y siga las instrucciones en pantalla. Deberá de cargar el fichero CSR descargado en el paso anterior.

Descargue un nuevo fichero .PEM con el certificado de Apple.

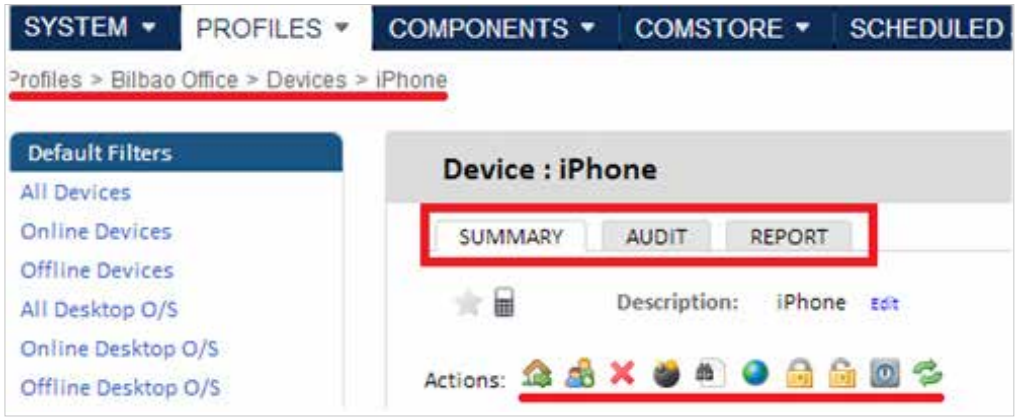
Cargue el nuevo fichero .PEM obtenido del Apple Push Certificate Portal en la **Consola PCSM**. Una vez cargado la consola tendrá un aspecto como el de la pantalla mostrada a continuación.



HERRAMIENTAS PARA LA GESTIÓN REMOTA DE DISPOSITIVOS MÓVILES

A continuación se detallan las herramientas disponibles desde la **Consola PCSM,** su modo de funcionamiento y sus beneficios asociados.

Las funcionalidades específicas de la **Consola PCSM** se muestran únicamente en el Nivel Device que se corresponde al dispositivo que queremos administrar. Al mostrar el dispositivo en la consola la Barra de acciones y la Barra de pestañas se adaptan de forma automática habilitando las nuevas acciones disponibles.



Borrado del dispositivo (Device Wipe)

Esta característica permite devolver el dispositivo a su estado original para prevenir el robo de información en caso de pérdida o sustracción, o ante casos de mal funcionamiento del terminal.

> Todos los datos personales del terminal, programas instalados por el usuario, configuraciones particulares y modificaciones se perderán de forma irreversible. El estado del terminal se revierte al original entregado de fabrica.

Geolocalización

Representa la posición del dispositivo en un mapa. Las coordenadas del dispositivo para situarlo en un punto del mapa son obtenidas de diferentes formas en función de los recursos disponibles del dispositivo, siendo muy variable su nivel de precisión. A continuación se listan las tecnologías soportadas, ordenadas de mayor a menor precisión.

- ✔ GPS (Global Positioning System)
- ✔ WPS (Wifi Position System)
- ✔ GeoIP

> Los dispositivos posicionados con GeoIP pueden aparecer en localizaciones totalmente diferentes a donde se encuentran realmente.

Bloqueo del dispositivo (Lock Device)

El bloqueo del dispositivo apaga la pantalla del dispositivo y si estaba establecido un PIN de seguridad se le solicitara de nuevo al usuario cuando active el móvil. Útil en caso de robo del terminal.

Desbloqueo del dispositivo (Unlock Device)

En el caso de que el usuario haya olvidado su contraseña esta funcionalidad resetea el PIN.

Política de contraseña (Password Policy)

Esta funcionalidad trabaja en conjunción con la de bloqueo del dispositivo ya que obliga al dueño del terminal a establecer una contraseña (PIN). Una vez establecida, el administrador podrá bloquear el dispositivo si es robado de forma que al encenderlo de nuevo se pedirá la contraseña establecida por su legítimo dueño.

> Esta funcionalidad lanza de forma remota un requerimiento al usuario para establecer el PIN, no permite al administrador establecerlo desde la consola.

Auditorias

Las auditorias funcionan de la misma manera que en dispositivos Windows quedando totalmente integradas en la **Consola PCSM**. De esta manera por ejemplo se pueden aplicar filtros a dispositivos móviles en base a los programas instalados.

El **Agente PCSM** instalado en el dispositivo móvil recaba toda la información de hardware y software y notifica los cambios al **Servidor PCSM**, que los muestra en la consola bajo la pestaña Audit.

El apartado Hardware muestra la información relevante del dispositivo móvil:

- ✔ Sistema operativo y versión
- ✔ Modelo
- ✔ ICCID (Integrated Circuit Card ID, identificador internacional de la SIM)
- ✔ Operador de la SIM instalada
- ✔ Número de teléfono de la SIM instalada
- ✔ Almacenamiento (memoria interna y SD instaladas)
- ✔ Adaptadores de red instalados (generalmente Wifi)

En el apartado Software se muestran todos los paquetes instalados en el terminal. En el apartado Changelog se muestran los cambios a nivel hardware y software que se han producido en el dispositivo móvil.

Informes

Los informes ofrecidos se adaptan al tipo de dispositivo. El comportamiento de la pestaña Reports es idéntico al del resto de dispositivos Windows y Mac.

16. APÉNDICE A

Código fuente del componente del capítulo 10

```
Option Explicit
'*****************************************************************
***
'Quarantine_Monitor v0.99b
'06/03/2013
'By Oscar Lopez / Panda Security
'Target: It monitors changes on PCOP quarantine folder
'Input: PCOP_PATH environment variable
'Output: stdout "Result=n new items detected in PCOP quarantine",
'n is the added file number in the monitored folder
'*****************************************************************
***

dim WshShell,WshSysEnv
dim objFSO,objFolder,colFiles
dim iCountPast,iCountNow
dim bHit
Dim n

Set WshShell = WScript.CreateObject("WScript.Shell")
Set objFSO = CreateObject("Scripting.FileSystemObject")

'access to environment variable and quarantine path
On error resume Next
    Set WshSysEnv = WshShell.Environment("PROCESS")
    Set objFolder = objFSO.GetFolder(WshSysEnv("PCOP_PATH"))
    if err.number <> 0 then
        'PCSM didn't send the environment variable
        err.clear
        WScript.Echo "<-Start Result->"
        WScript.Echo "Result=PCOP_
PATH variable not defined on PCSM console or path not found"
        WScript.Echo "<-End Result->"
        Set WshShell = nothing
        Set WshSysEnv = nothing
        Set objFolder = nothing
        WScript.Quit(1)
    end if
On error goto 0

'it gets the collection that contains the folter files
set colFiles = objFolder.files

On error resume text
    'access to the registry. 10 incremental entries will be crea-
ted, one per minute.
    n=0
    While Err.Number=0 And n < 10
        iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Securi-
ty\Monitor" & n))
        If err.number<>0 then
            WshShell.RegWrite "HKLM\Software\Panda Security\Moni-
tor" & n, colFiles.count, "REG_SZ"
```

```
Else
          n=n+1
       End If
    Wend
    Err.Clear

    If n=9 Then
       iCountPast= cint(WshShell.RegRead("HKLM\Software\Panda Securi-
ty\Monitor0"))
       iCountNow= cint(WshShell.RegRead("HKLM\Software\Panda Security\
Monitor9"))
       if iCountPast < iCountNow then
           'there is more items in the folder, it updates the regis-
triy and sends an alert
           WScript.Echo "<-Start Result->"
           WScript.Echo "Result=" & iCountNow - iCou-
ntPast & " new items in PCOP quarantine"
           WScript.Echo "<-End Result->"
           bHit=true
       end if
       For n=0 To 9
           WshShell.RegDelete("HKLM\Software\Panda Security\Moni-
tor" & n)
       Next
       WshShell.RegWrite "HKLM\Software\Panda Security\Monitor0", col-
Files.count, "REG_SZ"

    end if
On error goto 0

'finale
Set colFiles = nothing
set objFolder = nothing
set WshShell = nothing
set WshSysEnv = nothing
set objFSO = nothing

if bHit then
    WScript.Quit (1)
else
    WScript.Quit (0)
end if
```

17. APÉNDICE B

Código fuente del componente del capítulo 11

```
Option Explicit
'*********************************************************************
'Deploy_documents v0.99b
'12/03/2013
'By Oscar Lopez / Panda Security
'Target: It creates a folder int the user's desktop and copy on it the
'documents to deploy
'Entrada: files to copy
'Salida: error code or OK
'*********************************************************************
Dim CONST_PATH
Dim objFSO,objFolder,colFiles

'Maybe you want to use a global variable for this constant?
CONST_PATH="C:\ACME Documents"
On Error Resume Next
    Set objFSO=CreateObject("Scripting.FileSystemObject")
    Set objFolder = objFSO.Getfolder(CONST_PATH)
    If Err.Number=0 Then
        'the folder already exists, the files won't be copied
        WScript.Echo "Deploy unsuccessful: The folder already exists"
        WScript.Quit (0)
    End If

    'the folder will be created in the user's desktop
    Err.Clear
    Set objFolder = objFSO.CreateFolder(CONST_PATH)
    'the documents will be moved to the folder
    objFSO.MoveFile "doc1.docx", objFolder.Path & "\doc1.docx"
    objFSO.MoveFile "doc2.docx", objFolder.Path & "\doc2.docx"
    objFSO.MoveFile "doc3.docx", objFolder.Path & "\doc3.docx"
    If Err.Number<>0 Then
        WScript.Echo "Deploy unsuccessful: " & Err.Description
        WScript.Quit (1)
    Else
        WScript.Echo "Deploy successful: All files were copied"
        WScript.Quit (0)
    End If
On Error Goto 0
WScript.Quit (0)
```